Ministerio del Interior y Seguridad Pública

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

21-01-2022 | Año 4 | N°133

Boletín de Seguridad Cibernética

Semana del 14 al 20 de enero de 2022

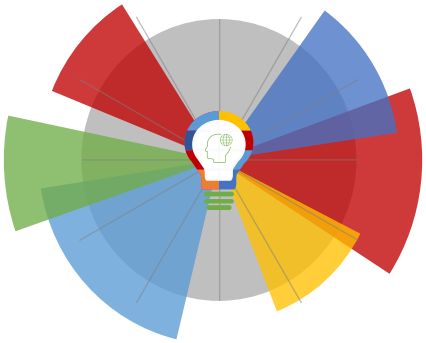
La semana en cifras

Hash

26

SHA

Asociadas a múltiples campañas de phishing con archivos que contienen malware



Se advirtieron

6

URL

Asociadas a sitios fraudulentos y campañas de phishing y malware.

Parches

28

para vulnerabilidades

Las mitigaciones son útiles en productos GitLab, Oracle, Wordpress, Drupal, SolarWinds y Trend Micro.

IP

24

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.

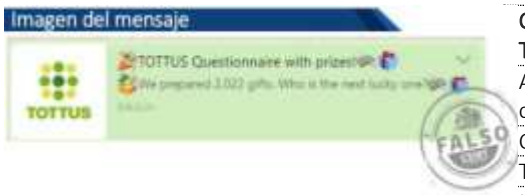
Contenido

Sitios fraudulentos

CSIRT advierte sitio fraudulento de la plataforma de correos Outlook	
Alerta de seguridad cibernética	8FFR21-01048-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	17 de enero de 2022
Última revisión	17 de enero de 2022
Indicadores de compromiso	
URL sitio falso	
hXXps://caiozzi[.]cl/cgi-bin/web-app/solutions/application/login/index.php	
IP	
[162.214.89.127]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr22-01048-01/	
https://www.csirt.gob.cl/media/2022/01/8FFR22-01048-01.pdf	

Phishing

CSIRT informa phishing que proviene supuestamente del Banco Ripley	
Alerta de seguridad cibernética	8FPH21-00464-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de enero de 2022
Última revisión	14 de enero de 2022
Indicadores de compromiso	
URL redirección	
hXXps://bit[.]ly/3tvNQ7g?l=www.bancoripley.cl	
hXXps://sspmprimaryschool[.]com/activacion/cuenta-ndln/	
URL sitio falso	
hXXps://wwwbancoripley-cl.mightytechs[.]in/1642101336/Login	
IP	
[194.233.72.106]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00464-01/	
https://www.csirt.gob.cl/media/2022/01/8FPH22-00464-01.pdf	



CSIRT advierte phishing con falso concurso del Supermercado Tottus	
Alerta de seguridad cibernética	8FPH21-00465-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	18 de enero de 2022
Última revisión	18 de enero de 2022
Indicadores de compromiso	
URL sitio falso	
https://superfluouscritic[.]top/m2l0Y0OC/tustot/?_t=1642529381207#1642529383319	
IP	
[104.21.45.96:]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00465-01/	
https://www.csirt.gob.cl/media/2022/01/8FPH22-00465-01-1.pdf	

CSIRT advierte phishing con falso concurso suplantando a a empresas Copec	
Alerta de seguridad cibernética	8FPH21-00466-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	20 de enero de 2022
Última revisión	20 de enero de 2022
Indicadores de compromiso	
URL sitio falso	
https://nkkvits[.]cn/PzDl4nXY/copec/?_t=1642676045354#1642676587928	
IP	
[172.67.198.200]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00466-01/	
https://www.csirt.gob.cl/media/2022/01/8FPH22-00466-01.pdf	

Vulnerabilidades

CSIRT comparte vulnerabilidades y mitigaciones para GitLab	
Alerta de seguridad cibernética	9VSA21-00550-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	17 de enero de 2022
Última revisión	17 de enero de 2022

CVE

CVE-2021-39946 - CVE-2022-0154 - CVE-2022-0152
CVE-2022-0151 - CVE-2022-0172 - CVE-2022-0090
CVE-2022-0125 - CVE-2022-0124 - CVE-2021-39942
CVE-2022-0093 - CVE-2021-39927

Fabricante

GitLab

Productos afectados

Edición de la comunidad de Gitlab: 7.7, 7.7.0, 7.7.1, 7.7.2, 7.8, 7.8.0, 7.8.1, 7.8.2, 7.8.3, 7.8.4, 7.9, 7.9.0, 7.9.1, 7.9.2, 7.9.3, 7.9.4, 7.10, 7.10.0, 7.10.1, 7.10.2, 7.10.3, 7.10.4, 7.10.5, 7.11, 7.11.0, 7.11.1, 7.11. 2, 7.11.3, 7.11.4, 7.12, 7.12.0, 7.12.1, 7.12.2, 7.13, 7.13.0, 7.13.1, 7.13.2, 7.13.3, 7.13.4, 7.13.5, 7.14, 7.14.0, 7.14.1, 7.14.2, 7.14.3, 8.0, 8.0.0, 8.0.1, 8.0.2, 8.0.3, 8.0.4, 8.0.5, 8.1, 8.1.0, 8.1.1, 8.1.2, 8.1.3, 8.1.4, 8.2, 8.2.0, 8.2.1, 8.2.2, 8.2.3, 8.2.4, 8.2.5, 8.2.6, 8.3, 8.3. 0, 8.3.1, 8.3.2, 8.3.3, 8.3.4, 8.3.5, 8.3.6, 8.3.7, 8.3.8, 8.3.9, 8.3.10, 8.4, 8.4.0, 8.4. 1, 8.4.2, 8.4.3, 8.4.4, 8.4.5, 8.4.6, 8.4.7, 8.4.8, 8.4.9, 8.4.10, 8.4.11, 8.5, 8.5.0, 8.5. 1, 8.5.2, 8.5.3, 8.5.4, 8.5.5, 8.5.6, 8.5.7, 8.5.8, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.6, 8.6.0, 8.6.1, 8.6.2, 8.6.3, 8.6.4, 8.6.5, 8.6.6, 8.6.7, 8.6.8, 8.6.9, 8.7, 8.7.0, 8.7.1, 8.7.2, 8.7.3, 8.7.4, 8.7.5, 8.7.6, 8.7.7, 8.7.8, 8.7.9, 8.8, 8.8.0, 8.8.1, 8.8. 2, 8.8.3, 8.8.4, 8.8.5, 8.8.6, 8.8.7, 8.8.8, 8.8.9, 8.9, 8.9.0, 8.9.1, 8.9.2, 8.9.3, 8.9. 4, 8.9.5, 8.9.6, 8.9.7, 8.9.8, 8.9.9, 8.9.10, 8.9.11, 8.10, 8.10.0, 8.10.1, 8.10.2, 8.10.3, 8.10. 4, 8.10.5, 8.10.6, 8.10.7, 8.10.8, 8.10.9, 8.10.10, 8.10.11, 8.10.12, 8.10.13, 8.11, 8.11.0, 8.11.1, 8.11. 2, 8.11.3, 8.11.4, 8.11.5, 8.11.6, 8.11.7, 8.11.8, 8.11.9, 8.11.10, 8.11.11, 8.12, 8.12.0, 8.12.1, 8.12. 2, 8.12.3, 8.12.4, 8.12.5, 8.12.6, 8.12.7, 8.12.8, 8.12.9, 8.12.10, 8.12.11, 8.12.12, 8.12.13, 8.13, 8.13. 0, 8.13.1, 8.13.2, 8.13.3, 8.13.4, 8.13.5, 8.13.6, 8.13.7, 8.13.8, 8.13.9, 8.13.10, 8.13.11, 8.13.12, 8.14, 8.14.0, 8.14.1, 8.14.2, 8.14.3, 8.14.4, 8.14.5, 8.14.6, 8.14.7, 8.14.8, 8.14.9, 8.14.10, 8.15, 8.15. 0, 8.15.1, 8.15.2, 8.15.3, 8.15.4, 8.15.5, 8.15.6, 8.15.7, 8.15.8, 8.16.0, 8.16.1, 8.16.2, 8.16.3, 8.16.4, 8.16.5, 8.16.6, 8.16.7, 8.16.8, 8.16.9, 8.17, 8.17.0, 8.17. 1, 8.17.2, 8.17.3, 8.17.4, 8.17.5, 8.17.6, 8.17.7, 8.17.8, 9.0, 9.0.0, 9.0.1, 9.0.2, 9.0.3, 9.0. 4, 9.0.5, 9.0.6, 9.0.7, 9.0.8, 9.0.9, 9.0.10, 9.0.11, 9.0.12, 9.0.13, 9.1, 9.1.0, 9.1.1, 9.1. 2, 9.1.3, 9.1.4, 9.1.5, 9.1.6, 9.1.7, 9.1.8, 9.1.9, 9.1.10, 9.2, 9.2.0, 9.2.1, 9.2.2, 9.2. 3, 9.2.4, 9.2.5, 9.2.6, 9.2.7, 9.2.8, 9.2.9, 9.2.10, 9.3, 9.3.0, 9.3.1, 9.3.2, 9.3.3, 9.3. 4, 9.3.5, 9.3.6, 9.3.7, 9.3.8, 9.3.9, 9.3.10, 9.3.11, 9.4, 9.4.0, 9.4.1, 9.4.2, 9.4.3, 9.4. 4, 9.4.5, 9.4.6, 9.4.7, 9.5, 9.5.0, 9.5.1, 9.5.2, 9.5.3, 9.5.4, 9.5.5, 9.5.6, 9.5.7, 9.5. 8, 9.5.9, 9.5.10, 9.55, 10.0, 10.0.0, 10.0.1, 10.0.2,

10.0.3, 10.0.4, 10.0.5, 10.0.6, 10.0.7, 10.1, 10.1. 0, 10.1.1, 10.1.2, 10.1.3, 10.1.4, 10.1.5, 10.1.6, 10.1.7, 10.2, 10.2.0, 10.2.1, 10.2.2, 10.2.3, 10.2.4, 10.2.5, 10.2.6, 10.2.7, 10.2.8, 10.3, 10.3.0, 10.3.1, 10.3.2, 10.3.3, 10.3.4, 10.3.5, 10.3.6, 10.3. 7, 10.3.8, 10.3.9, 10.4, 10.4.0, 10.4.1, 10.4.2, 10.4.3, 10.4.4, 10.4.5, 10.4.6, 10.4.7, 10.5, 10.5.0, 10.5.1, 10.5.2, 10.5.3, 10.5.4, 10.5.5, 10.5.6, 10.5.7, 10.5.8, 10.6, 10.6.0, 10.6.1, 10.6.2, 10.6.3, 10.6.4, 10.6.5, 10.6.6, 10.7, 10.7.0, 10.7.1, 10.7.2, 10.7.3, 10.7.4, 10.7.5, 10.7.6, 10.7.7, 10.8, 10.8. 0, 10.8.1, 10.8.2, 10.8.3, 10.8.4, 10.8.5, 10.8.6, 10.8.7, 11.0, 11.0.0, 11.0.1, 11.0.2, 11.0.3, 11.0. 4, 11.0.5, 11.0.6, 11.1, 11.1.0, 11.1.1, 11.1.2, 11.1.3, 11.1.4, 11.1.5, 11.1.6, 11.1.7, 11.1.8, 11.2, 11.2.0, 11.2.1, 11.2.2, 11.2.3, 11.2.4, 11.2.5, 11.2.6, 11.2.7, 11.2.8, 11.3, 11.3.0, 11.3.1, 11.3.2, 11.3.3, 11.3.4, 11.3.5, 11.3.6, 11.3.7, 11.3.8, 11.3.9, 11.3.10, 11.3.11, 11.3.12, 11.3.13, 11.3.14, 11.4, 11.4.0, 11.4.1, 11.4.2, 11.4.3,11.4.4, 11.4.5, 11.4.6, 11.4.7, 11.4.8, 11.4.9, 11.4.10, 11.4.11, 11.4.12, 11.4.13, 11.4.14, 11.5.0, 11.5. 1, 11.5.2, 11.5.3, 11.5.4, 11.5.5, 11.5.6, 11.5.7, 11.5.8, 11.5.9, 11.5.10, 11.5.11, 11.6.0, 11.6.1, 11.6.2, 11.6.3, 11.6.4, 11.6.5, 11.6.6, 11.6.7, 11.6.8, 11.6.9, 11.6.10, 11.6.11, 11.7.0, 11.7.1, 11.7. 2, 11.7.3, 11.7.4, 11.7.5, 11.7.6, 11.7.7, 11.7.8, 11.7.9, 11.7.10, 11.7.11, 11.7.12, 11.8.0, 11.8.1, 11.8.2, 11.8.3, 11.8.4, 11.8.5, 11.8.6, 11.8.7, 11.8.8, 11.8.9, 11.8.10, 11.9.0, 11.9.1, 11.9.2, 11.9. 3, 11.9.4, 11.9.5, 11.9.6, 11.9.7, 11.9.8, 11.9.9, 11.9.10, 11.9.11, 11.9.12, 11.10.0, 11.10.1, 11.10.2, 11.10.3, 11.10.4, 11.10.5, 11.10.6, 11.10.7, 11.10.8, 11.11.0, 11.11.1, 11.11.2, 11.11.3, 11.11.4, 11.11.5, 11.11. 7, 11.11.8, 12.0.0, 12.0.1, 12.0.2, 12.0.3, 12.0.4, 12.0.6, 12.0.8, 12.0.9, 12.0.10, 12.0.12, 12.1.0, 12.1.1, 12.1.2, 12.1.3, 12.1.4, 12.1.6, 12.1.8, 12.1.9, 12.1.10, 12.1.11, 12.1.12, 12.1.13, 12.1.14, 12.1.15, 12.1.16, 12.1.17, 12.2. 0, 12.2.1, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7, 12.2.8, 12.2.9, 12.2.10, 12.2.11, 12.2.12, 12.3.0, 12.3.1, 12.3.2, 12.3.3, 12.3.4, 12.3.5, 12.3.6, 12.3.7, 12.3.8, 12.3.9, 12.4.0, 12.4.1, 12.4.2, 12.4. 3, 12.4.4, 12.4.5, 12.4.6, 12.4.7, 12.4.8, 12.5.0, 12.5.1, 12.5.2, 12.5.3, 12.5.4, 12.5.5, 12.5.6, 12.5.7, 12.5.9, 12.5.10, 12.6.0, 12.6.1, 12.6.2, 12.6.3, 12.6.4, 12.6.6, 12.6.7, 12.6.8, 12.7.0, 12.7. 1, 12.7.2, 12.7.4, 12.7.5, 12.7.6, 12.7.7, 12.7.8, 12.7.9, 12.8.0, 12.8.1, 12.8.2, 12.8.3, 12.8.4, 12.8.5, 12.8.6, 12.8.7, 12.8.8, 12.8.9, 12.8.10, 12.9.0, 12.9.1, 12.9.2, 12.9.3, 12.9.4, 12.9.5, 12.9. 6, 12.9.7, 12.9.8, 12.9.9, 12.9.10, 12.10.0, 12.10.1, 12.10.2, 12.10.3, 12.10.4, 12.10.5, 12.10.6, 12.10.7, 12.10.8, 12.10.9, 12.10.10, 12.10.11,12.10.12, 12.10.13, 12.10.14, 13.0.0, 13.0.1, 13.0.2, 13.0.3, 13.0.4, 13.0.5, 13.0.6, 13.0.7, 13.0.8, 13.0. 9, 13.0.10, 13.0.12, 13.0.13, 13.0.14, 13.1.0, 13.1.1, 13.1.2, 13.1.3, 13.1.4, 13.1.5, 13.1.6, 13.1.7, 13.1.8, 13.1.9, 13.1.10, 13.1.11, 13.2.0, 13.2.1, 13.2.2, 13.2.3, 13.2.4, 13.2.5, 13.2.6, 13.2.7, 13.2. 8, 13.2.9, 13.2.10, 13.3.0, 13.3.1, 13.3.2, 13.3.3, 13.3.4, 13.3.5, 13.3.6, 13.3.7, 13.3.8, 13.3.9, 13.4.0, 13.4.1, 13.4.2, 13.4.3, 13.4.4, 13.4.5, 13.4.6, 13.4.7, 13.5.0, 13.5.1, 13.5.2, 13.5.3, 13.5. 4, 13.5.5, 13.5.6, 13.5.7, 13.6.0, 13.6.1, 13.6.2, 13.6.3, 13.6.4, 13.6.5, 13.6.6, 13.6.7, 13.7.0, 13.7.1, 13.7.2, 13.7.3, 13.7.4, 13.7.5, 13.7.6, 13.7.7, 13.7.8, 13.7.9, 13.8.0, 13.8.1, 13.8.2, 13.8. 3, 13.8.4, 13.8.5, 13.8.6, 13.8.7, 13.8.8, 13.9.0, 13.9.1, 13.9.2, 13.9.3, 13.9.4, 13.9.5, 13.9.6, 13.9.7, 13.10.0, 13.10.1, 13.10.2, 13.10.3,13.10.4, 13.10.5, 13.11.0, 13.11.1, 13.11.2, 13.11.3, 13.11.4, 13.11.5, 13.11.6, 13.11.7, 13.12.0, 13.12.1, 13.12. 2, 13.12.3, 13.12.4, 13.12.5, 13.12.6, 13.12.7, 13.12.8, 13.12.9, 13.12.10, 13.12.11, 14.0.0, 14.0.1, 14.0.2, 14.0.3, 14.0.4, 14.0.5, 14.0.6, 14.0.7, 14.0.8,

14.0.9, 14.0.10, 14.1.0, 14.1.1, 14.1.2, 14.1.3, 14.1. 4, 14.1.5, 14.1.6, 14.1.7, 14.2.0, 14.2.1, 14.2.2, 14.2.3, 14.2.5, 14.2.6, 14.3.0, 14.3.1, 14.3.2, 14.3.3, 14.3.4, 14.3.5, 14.3.6, 14.4.0, 14.4.1, 14.4.2, 14.4.3, 14.4. 4, 14.5.0, 14.5.1, 14.5.2, 14.6. 0, 14.6.14, 14.1.5, 14.1.6, 14.1.7, 14.2.0, 14.2.1, 14.2.2, 14.2.3, 14.2.5, 14.2.6, 14.3.0, 14.3.1, 14.3.2, 14.3.3, 14.3.4, 14.3.5, 14.3.6, 14.4.0, 14.4.1, 14.4.2, 14.4.3, 14.4.4, 14.5.0, 14.5.1, 14.5.2, 14.6. 0, 14.6.14, 14.1.5, 14.1.6, 14.1.7, 14.2.0, 14.2.1, 14.2.2, 14.2.3, 14.2.5, 14.2.6, 14.3.0, 14.3.1, 14.3.2, 14.3.3, 14.3.4, 14.3.5, 14.3.6, 14.4.0, 14.4.1, 14.4.2, 14.4.3, 14.4.4, 14.5.0, 14.5.1, 14.5.2, 14.6. 0, 14.6.1

GitLab Enterprise Edition: 7.7.0, 7.8.0, 7.9.0, 7.10.0, 7.10.1, 7.11.0, 7.11.2, 7.11.3, 7.11.4, 7.12.0, 7.12.1, 7.12. 2, 7.13.0, 7.13.1, 7.13.2, 7.13.3, 7.14.0, 7.14.1, 7.14.2, 7.14.3, 8.0.0, 8.0.1, 8.0.2, 8.0.3, 8.0.4, 8.0.5, 8.0.6, 8.1.0, 8.1.1, 8.1.2, 8.1.3, 8.1.4, 8.2.0, 8.2.1, 8.2.2, 8.2.3, 8.2. 4, 8.2.5, 8.2.6, 8.3.0, 8.3.1, 8.3.2, 8.3.3, 8.3.4, 8.3.5, 8.3.6, 8.3.7, 8.3.8, 8.3.9, 8.3.10, 8.4.0, 8.4.1, 8.4.2, 8.4.3, 8.4.4, 8.4.5, 8.4.6, 8.4.7, 8.4.8, 8.4.9, 8.4.10, 8.4. 11, 8.5.0, 8.5.1, 8.5.2, 8.5.3, 8.5.4, 8.5.5, 8.5.6, 8.5.7, 8.5.8, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.6.0, 8.6.1, 8.6.2, 8.6.3, 8.6.4, 8.6.5, 8.6.6, 8.6.7, 8.6.8, 8.6.9, 8.7. 0, 8.7.1, 8.7.2, 8.7.3, 8.7.4, 8.7.5, 8.7.6, 8.7.7, 8.7.8, 8.7.9, 8.8.0, 8.8.1, 8.8.2, 8.8.3, 8.8.4, 8.8.5, 8.8.6, 8.8.7, 8.8.8, 8.8.9, 8.9.0, 8.9.1, 8.9.2, 8.9.3, 8.9.4, 8.9. 5, 8.9.6, 8.9.7, 8.9.8, 8.9.9, 8.9.10, 8.10.0, 8.10.1, 8.10.2, 8.10.3, 8.10.4, 8.10.5, 8.10.6, 8.10.7, 8.10.8, 8.10.9, 8.10.10, 8.10.11, 8.10.12, 8.11.0, 8.11.1, 8.11.2, 8.11.3, 8.11.4, 8.11.5, 8.11.6, 8.11.7, 8.11.8, 8.11.9, 8.11. 10, 8.11.11, 8.12.0, 8.12.1, 8.12.2, 8.12.3, 8.12.4, 8.12.5, 8.12.6, 8.12.7, 8.12.8, 8.12.9, 8.12.10, 8.12.11, 8.12.12, 8.13.0, 8.13.1, 8.13.2, 8.13.3, 8.13.4, 8.13.5, 8.13.6, 8.13.7, 8.13.8, 8.13.9, 8.13. 10, 8.13.11, 8.13.12, 8.14.0, 8.14.1, 8.14.2, 8.14.3, 8.14.4, 8.14.5, 8.14.6, 8.14.7, 8.14.8, 8.14.9, 8.14.10, 8.15.0, 8.15.1, 8.15.2, 8.15.3, 8.15.4, 8.15.5, 8.15.6, 8.15.7, 8.15.8, 8.16.0, 8.16.1, 8.16. 2, 8.16.3, 8.16.4, 8.16.5, 8.16.6, 8.16.7, 8.16.8, 8.16.9, 8.17.0, 8.17.1, 8.17.2, 8.17.3, 8.17.4, 8.17.5, 8.17.6, 8.17.7, 8.17.8, 9.0.0, 9.0.1, 9.0.2, 9.0.3, 9.0.4, 9.0.5, 9.0.6, 9.0.7, 9.0. 8, 9.0.9, 9.0.10, 9.0.11, 9.0.12, 9.0.13, 9.1.0, 9.1.1, 9.1.2, 9.1.3, 9.1.4, 9.1.5, 9.1.6, 9.1.7, 9.1.8, 9.1.9, 9.1.10, 9.2.0, 9.2.1, 9.2.2, 9.2. 3, 9.2.4, 9.2.5, 9.2.6, 9.2.7, 9.2.8, 9.2.9, 9.2.10, 9.3.0, 9.3.1, 9.3.2, 9.3.3, 9.3.4, 9.3.5, 9.3.6, 9.3.7, 9.3.8, 9.3.9, 9.3.10, 9.3.11, 9.4.0, 9.4.1, 9.4.2, 9.4.3, 9.4.4, 9.4. 5, 9.4.6, 9.4.7, 9.5.0, 9.5.1, 9.5.2, 9.5.3, 9.5.4, 9.5.5, 9.5.6, 9.5.7, 9.5.8, 9.5.9, 9.5.10, 10.0.0, 10.0.1, 10.0.2, 10.0.3, 10.0.4, 10.0.5, 10.0.7, 10.1.0, 10.1.1, 10.1.2, 10.1.3, 10.1. 4, 10.1.5, 10.1.6, 10.1.7, 10.2.0, 10.2.1, 10.2.2, 10.2.3, 10.2.4, 10.2.5, 10.2.6, 10.2.7, 10.2.8, 10.3.0, 10.3.1, 10.3.2, 10.3.3, 10.3.4, 10.3.5, 10.3.6, 10.3.7, 10.3.8, 10.3.9, 10.4.0, 10.4.1, 10.4. 2, 10.4.3, 10.4.4, 10.4.5, 10.4.6, 10.4.7, 10.5.0, 10.5.1, 10.5.2, 10.5.3, 10.5.4, 10.5.5, 10.5.6, 10.5.7, 10.5.8, 10.6.0, 10.6.1, 10.6.2, 10.6.3, 10.6.4, 10.6.5, 10.6.6, 10.7.0, 10.7.1, 10.7.2, 10.7. 3,10.7.4, 10.7.5, 10.7.6, 10.7.7, 10.8.0, 10.8.1, 10.8.2, 10.8.3, 10.8.4, 10.8.5, 10.8.6, 11.0.0, 11.0. 1, 11.0.2, 11.0.3, 11.0.4, 11.0.5, 11.0.6, 11.1.0, 11.1.1, 11.1.2, 11.1.3, 11.1.4, 11.1.5, 11.1.6, 11.1.7, 11.2.0, 11.2.1, 11.2.2, 11.2.3, 11.2.4, 11.2.5, 11.2.6, 11.2.7, 11.2.8, 11.3.0, 11.3.1, 11.3. 2, 11.3.3, 11.3.4, 11.3.5, 11.3.6, 11.3.7, 11.3.8, 11.3.9, 11.3.10, 11.3.11, 11.3.13, 11.3.14, 11.4.0, 11.4.1, 11.4.2, 11.4.3, 11.4.4, 11.4.5, 11.4.6, 11.4.7, 11.4.8, 11.4.9, 11.5.0, 11.5.1, 11.5.2, 11.5. 3, 11.5.5, 11.5.8, 11.5.10, 11.5.11, 11.6.0, 11.6.1, 11.6.2, 11.6.3, 11.6.4, 11.6.5, 11.6.8, 11.6.9, 11.6.10, 11.6.11, 11.7.0, 11.7.1, 11.7.2, 11.7.3, 11.7.5,

11.7.7, 11.7.8, 11.7.10, 11.7.11, 11.7.12, 11.8. 0, 11.8.2, 11.8.3, 11.8.6, 11.8.7, 11.8.10, 11.9.0, 11.9.1, 11.9.2, 11.9.3, 11.9.5, 11.9.6, 11.9.7, 11.9.8, 11.9.9, 11.9.10, 11.9.12, 11.10.0, 11.10.1, 11.10.2, 11.10.3, 11.10.4, 11.10.6, 11.10.7, 11.10.8, 11.11.0, 11.11.2, 11.11.3, 11.11.4, 11.11.7, 11.11.8, 12.0.0, 12.0.1, 12.0.2, 12.0.6, 12.0.7, 12.0.9, 12.0.10, 12.0.12, 12.1.1, 12.1.2, 12.1.3, 12.1.4, 12.1. 5, 12.1.9, 12.1.10, 12.1.12, 12.1.14, 12.2.0, 12.2.1, 12.2.2, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7, 12.2.8, 12.2.11, 12.3.0, 12.3.1, 12.3.2, 12.3.4, 12.3.7, 12.3.9, 12.4.0, 12.4.1, 12.4.2, 12.4.3, 12.4. 5, 12.4.8, 12.5.0, 12.5.1, 12.5.3, 12.5.4, 12.5.5, 12.5.8, 12.5.9, 12.6.0, 12.6.1, 12.6.2, 12.6.4, 12.6.5, 12.6.6, 12.6.7, 12.7.0, 12.7.1, 12.7.2, 12.7.3, 12.7.4, 12.7.5, 12.7.9, 12.8.0, 12.8.1, 12.8. 2, 12.8.3, 12.8.4, 12.8.5, 12.8.6, 12.8.7, 12.8.9, 12.8.10, 12.9.0, 12.9.1, 12.9.2, 12.9.3, 12.9.4, 12.9.5, 12.9.6, 12.9.8, 12.9.10, 12.10.0, 12.10.1, 12.10.2, 12.10.4, 12.10.5, 12.10.6, 12.10.7, 12.10.8, 12.10. 11, 12.10.12, 12.10.13, 12.10.14, 13.0.0, 13.0.1, 13.0.3, 13.0.4, 13.0.6, 13.0.7, 13.0.8, 13.0.9, 13.0.10, 13.0.11, 13.0.12, 13.0.13, 13.0.14, 13.1.0, 13.1.1, 13.1.2, 13.1.3, 13.1.5, 13.1.6, 13.1.7, 13.1.8, 13.1.9, 13.1.10, 13.2.0, 13.2. 2, 13.2.3, 13.2.4, 13.2.5, 13.2.6, 13.2.7, 13.2.8, 13.2.10, 13.3.0, 13.3.1, 13.3.2, 13.3.3, 13.3.4, 13.3.5, 13.3.6, 13.3.7, 13.3.8, 13.3.9, 13.4.0, 13.4.2, 13.4.3, 13.4.4, 13.4.5, 13.4.6, 13.4.7, 13.5. 0, 13.5.1, 13.5.2, 13.5.3, 13.5.4, 13.5.5, 13.5.6, 13.5.7, 13.6.0, 13.6.1, 13.6.2, 13.6.3, 13.6.4, 13.6.5, 13.6.6, 13.6.7, 13.7.0, 13.7.1, 13.7.2, 13.7.3, 13.7.4, 13.7.5, 13.7.6, 13.7.7, 13.7.8, 13.7. 9, 13.8.0, 13.8.1, 13.8.2, 13.8.3, 13.8.4, 13.8.5, 13.8.6, 13.8.7, 13.8.8, 13.9.0, 13.9.1, 13.9.2, 13.9.3, 13.9.4, 13.9.5, 13.9.6, 13.9.7, 13.10.0, 13.10.1, 13.10.2, 13.10.3, 13.10.4, 13.10.5, 13.11.0, 13.11. 1, 13.11.2, 13.11.3, 13.11.4, 13.11.5,13.11.6, 13.11.7, 13.12.0, 13.12.1, 13.12.2, 13.12.3, 13.12.4, 13.12.5, 13.12.6, 13.12.7, 13.12.8, 13.12.9, 13.12. 10, 13.12.11, 13.12.12, 13.12.13, 13.12.14, 13.12.15, 14.0.0, 14.0.1, 14.0.2, 14.0.3, 14.0.4, 14.0.5, 14.0.6, 14.0.7, 14.0.8, 14.0.9, 14.0.10, 14.0.11, 14.0.12, 14.1.0, 14.1.1, 14.1.2, 14.1.3, 14.1.4, 14.1.5, 14.1. 6, 14.1.7, 14.1.8, 14.2.0, 14.2.1, 14.2.2, 14.2.3, 14.2.4, 14.2.5, 14.2.6, 14.2.7, 14.3.0, 14.3.1, 14.3.2, 14.3.3, 14.3.4, 14.3.5, 14.3.6, 14.4.0, 14.4.1, 14.4.2, 14.4.3, 14.4.4, 14.5.0, 14.5.1, 14.5. 2, 14.6.0, 14.6.114.1.5, 14.1.6, 14.1.7, 14.1.8, 14.2.0, 14.2.1, 14.2.2, 14.2.3, 14.2.4, 14.2.5, 14.2.6, 14.2.7, 14.3. 0, 14.3.1, 14.3.2, 14.3.3, 14.3.4, 14.3.5, 14.3.6, 14.4.0, 14.4.1, 14.4.2, 14.4.3, 14.4.4, 14.5.0, 14.5.1, 14.5.2, 14.6.0, 14.6.114.1.5, 14.1.6, 14.1.7, 14.1.8, 14.2.0, 14.2.1, 14.2.2, 14.2.3, 14.2.4, 14.2.5, 14.2.6, 14.2.7, 14.3. 0, 14.3.1, 14.3.2, 14.3.3, 14.3.4, 14.3.5, 14.3.6, 14.4.0, 14.4.1, 14.4.2, 14.4.3, 14.4.4, 14.5.0, 14.5.1, 14.5.2, 14.6.0, 14.6.1
Enlaces para revisar el informe:
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00550-01/
https://www.csirt.gob.cl/media/2022/01/9VSA21-00550-01.pdf

CSIRT comparte vulnerabilidades de tres complementos de WordPress	
Alerta de seguridad cibernética	9VSA21-00551-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	18 de enero de 2022
Última revisión	18 de enero de 2022
CVE	
CVE-2022-0215	
Fabricante	
Wordpress	
Productos afectados	
<= 2.2 en la ventana emergente de Login/Signup Popup. <= 2.5.1 en Waitlist Woocommerce. <= 2.0 en Side Cart Woocommerce (Ajax).	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00551-01/	
https://www.csirt.gob.cl/media/2022/01/9VSA22-00551-01-1.pdf	

CSIRT informa de vulnerabilidades en Oracle Utilities Testing Accelerator	
Alerta de seguridad cibernética	9VSA21-00552-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	19 de enero de 2022
Última revisión	19 de enero de 2022
CVE	
CVE-2021-29425 - CVE-2021-33037 - CVE-2021-36374 CVE-2021-4104 - CVE-2021-36090 - CVE-2021-22118 CVE-2021-2351 - CVE-2021-39139 - CVE-2020-13936	
Fabricante	
Oracle	
Productos afectados	
Versiones: 6.0.0.1.1, 6.0.0.2.2, 6.0.0.3.1	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00552-01/	
https://www.csirt.gob.cl/media/2022/01/9VSA22-00552-01.pdf	

CSIRT comparte múltiples vulnerabilidades en la biblioteca JS de Drupal	
Alerta de seguridad cibernética	9VSA21-00553-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	19 de enero de 2022
Última revisión	19 de enero de 2022
CVE	
CVE-2021-41182 CVE-2021-41183 CVE-2016-7103 CVE-2010-5312	
Fabricante	
Drupal	
Productos afectados	
Versiones: 7.0, 7.1, 7.1-1.2, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 7.9, 7.10, 7.11, 7.12, 7.13, 7.14, 7.15, 7.16, 7.17, 7.18, 7.19, 7.2.2 7.22, 7.23, 7.24, 7.23, 7.26, 7.25, 7.28, 7.27, 7.28, 7.29, 7.30, 7.31, 7.32, 7.33, 7.34, 7.35, 7.36, 7.37, 7.38, 7.39, 7.40, 7.41, 7.42, 7.43, 7.44, 7.50, 7.51, 7.50, 7.51, 7.52, 7.53, 7.54, 7.55, 7.56, 7.57, 7.58, 7.57, 7.58, 7.59, 7.60, 7.61, 7.62, 7.63, 7.64, 7.65, 7.66, 7.67, 7.68, 7.69, 7.70, 7.71, 7.72, 7.73, 7.74, 7.75, 7.76, 7.76, 7.77, 7.78, 7.79, 7.80, 7.81, 7.82, 7.83, 7.84, 7.85, 7.x, 7.x-1.0, 7.x-1.1, 7.x-1.2, 7.x-1.3, 7.x- 1.4, 7.x-dev	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00553-01/	
https://www.csirt.gob.cl/media/2022/01/9VSA22-00553-01.pdf	

CSIRT comparte vulnerabilidades y mitigaciones de Trend Micro	
Alerta de seguridad cibernética	9VSA21-00554-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	19 de enero de 2022
Última revisión	19 de enero de 2022
CVE	
CVE-2022-23119 CVE-2022-23120	
Fabricante	
Trend Micro	
Productos afectados	
10.0, 10.0 U1, 10.0 U2, 10.0 U3, 10.0 U4, 10.0 U5, 10.0 U6, 10.0 U7, 10.0 U8, 10.0 U9, 10.0 U10, 10.0 U11, 10.0 U12, 10.0 U13, 10.0 U14, 10.0 U14 10.0 U16, 10.0 U17, 10.0 U18, 10.0 U19, 10.0 U20, 10.0 U21, 10.0 U22, 10.0 U23, 10.0 U24, 10.0 U28, 10.0 U26, 10.0 U27, 10.0 U28, 10.0 U29, 10.0 U30, 10.0 U31, 10.1 (Versión de funciones), 11.0, 11.0 U1, 11.0 U2, 11.0 U3, 11.0 U4,	

11.0 U5, 11.0 U6, 11.0 U7, 11.0 U8, 11.0 U9, 11.0 U10, 11.0 U11, 11.0 U12, 11.0 U13, 11.0 U014, 11.0 11.0 U16, 11.0 U17, 11.0 U18, 11.0 U19, 11.0 U20, 11.0 U21, 11.0 U22, 11.0 U23, 11.0 U24, 11.0 U25, 11.0 U26, 11.0 U27, 12.0, 12.0 U0.10, 12.0 U0. , 12.0 U5, 12.0 U6, 12.0 U7, 12.0 U8, 12.0 U9, 12.0 U10, 12.0 U11, 12.0 U12, 12.0 U13, 12.0 U14, 12.0 U15, 12.0 U16, 12.0 U17, 12.0 U18, 1.0, 12.0 U21, 20,0 LTS
Enlaces para revisar el informe:
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00554-01/
https://www.csirt.gob.cl/media/2022/01/9VSA22-00554-01.pdf

CSIRT advierte vulnerabilidad en la plataforma SolarWinds	
Alerta de seguridad cibernética	9VSA21-00555-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	20 de enero de 2022
Última revisión	20 de enero de 2022
CVE	
CVE-2021-35247	
Fabricante	
Trend Micro	
Productos afectados	
15.2.5 y versiones anteriores	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00555-01/	
https://www.csirt.gob.cl/media/2022/01/9VSA22-00555-01.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	N°Documento
32d44eccf7bc0c54b56a06ae8613fb336acb58d45bc901e0a6f73c9aad25ed74	MSIL/Kryptik	2CMV21-00267-01
0ced157a9989624a11b713d3f20b9bbaf6d110258d0a5540b69a785263f1b99d	MSIL/CoinMiner	2CMV21-00267-01
654ee607a193d7d3bf2ece94aa9af3478dc4bcc220b54872f3db69ae7dc7fd6f	MSIL/GenKryptik	2CMV21-00267-01
a1578bda0b28e1f7964f006c7b873543114cd0ab6c4e22cae5419ed74a9798a3	MSIL/GenKryptik	2CMV21-00267-01
4f235e7d96f7caf333c0a2cff4f6a860ac7ffca62918e2ddddb64cd10ed3ca94	MSIL/GenKryptik	2CMV21-00267-01
c1391e445b4c4888009f79c513da19ae1f846faaafa2bd4779aa96f8301496bd	MSIL/GenKryptik	2CMV21-00267-01
afaf29e3caa6f81224cc42933d966bf27481c040a8ed88fe9ebb9ba130f668cd	MSIL/CoinMiner	2CMV21-00267-01
e6471b3bf587c95aecd1bb4d4fa6b341797f3e41402c68b91eebd514c1cc2869	MSIL/GenKryptik	2CMV21-00267-01
d40dda28eb3ae29bfb4b88992d3f93dd11c6f909210ddcadfcf9f2aacb196b98	Malware_Generic	2CMV21-00267-01
3c200afc123f4ec9fea4c8e52de22de7229ca0d92c2771db597428c333b28712	MSIL/GenKryptik	2CMV21-00267-01
c9773c2c3db8a09f33f5ba35afee2d036283b0a302cfda97835e721d3e4ac7af	W32/Kryptik	2CMV21-00267-01
3bfedf5f7c37324a394a535d912f3dcb91c5934e843e4b610587906363db3223	MSIL/GenKryptik	2CMV21-00267-01
abfda6109651f6dcfcd50655890aaee6ff1a3ced119d925d20af186677098ccd	Riskware/POC_Iframe_CID	2CMV21-00267-01
e34317bb799040db5ac6d4821d19f6d0b9dba1ed1151217f3af0cd4ff1cde887	W32/Netsky	2CMV21-00267-01
86c54c0fe5904c2fc1991cfc5e286c00f7a399c2ff6a479c9d0193beb4abbb35	Malicious_Behavior	2CMV21-00267-01
7433e1df9f8d45fe6cc344aabee0f86d1d4968b8f910032e2c33fa8a2cf07ddf	HTML/Phishing	2CMV21-00267-01
095f1af7b4e88e0ab825190478738d0e02744cd553ec0e56989c8453a3607520	HTML/Phishing	2CMV21-00267-01
ac53397794de90ff6d4a3f0dca9fe0461e4b84aaa836bd70a94d418f6de7eaca	HTML/Phishing	2CMV21-00267-01
5b72fc57cf22b55a088f83fbf915cf63ff052a40cda34c589ed9e3fa53bbaa28	MSIL/GenKryptik	2CMV21-00267-01
31e8cba4a858778fefd770d93f4e5d41852248c43aae3d264f9f4c75e6d4a31c	HTML/Phishing	2CMV21-00267-01
20f0cfdf5c92f5b86cebde96452ea43997ba12148c2873c7c0c8141aa63e5f44	HTML/Phishing	2CMV21-00267-01
277f40f9cc9dfaba9ec68c0831973f287ff802c47c49d3278aaff86030c63b5a	HTML/Phishing	2CMV21-00267-01
380293b9c765ae6d40351bd50a9bba8e85fcdd8f4f7fe133f422488847f0d158	HTML/Phishing	2CMV21-00267-01
af888cc7c0eddb88526d5445743ad61a669d6c88d94d874eef4f8a876689dad6	MSIL/GenKryptik	2CMV21-00267-01
af246e9ccbefacfb89655a929007c1d2fe37aaefbbe537c020f48e41f2b692d6	MSIL/GenKryptik	2CMV21-00267-01
8a0961654c71edaffd006ad55de0d0c753f160402ad71c6cb89c220907a105ad	MSOffice/CVE_2017_11882	2CMV21-00267-01

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
88.30.17.247	Telefonica De Espana	2CMV21-00267-01
45.137.22.60	RootLayer Web Services Ltd.	2CMV21-00267-01
45.137.22.124	RootLayer Web Services Ltd.	2CMV21-00267-01
212.193.30.66	Delis LLC	2CMV21-00267-01
212.192.246.74	AS-SERVERION	2CMV21-00267-01
212.192.246.31	AS-SERVERION	2CMV21-00267-01
212.192.241.70	AS-SERVERION	2CMV21-00267-01
200.66.65.23	Megacable Comunicaciones de Mexico, S.A. de C.V.	2CMV21-00267-01
192.227.191.17	AS-COLOCROSSING	2CMV21-00267-01
192.227.191.16	AS-COLOCROSSING	2CMV21-00267-01
185.222.57.93	RootLayer Web Services Ltd.	2CMV21-00267-01
185.222.57.168	RootLayer Web Services Ltd.	2CMV21-00267-01
170.39.212.175	TIER-NET	2CMV21-00267-01
165.22.67.71	DIGITALOCEAN-ASN	2CMV21-00267-01
103.166.183.38	VIETNAM POSTS AND TELECOMMUNICATIONS GROUP	2CMV21-00267-01
103.156.93.66	VIETNAM POSTS AND TELECOMMUNICATIONS GROUP	2CMV21-00267-01
103.156.91.24	VIETNAM POSTS AND TELECOMMUNICATIONS GROUP	2CMV21-00267-01
212.192.246.250	AS-SERVERION	2CMV21-00267-01
212.192.246.202	AS-SERVERION	2CMV21-00267-01
23.235.223.116	INMOTION	2CMV21-00267-01

Nombres de archivo: Corresponden a aquellos documentos que vienen adjuntos en las campañas de phishing con malware. El CSIRT de Gobierno recomienda que cada institución analice las extensiones de los archivos y evalúe cuáles serán bloqueadas o permitidas. Asimismo se deben ejecutar de forma permanente las actualizaciones de los módulos de antivirus de los antispam y de las estaciones de trabajo.

Nombres de archivos con malware	Documento web
awb purchase order.html	2CMV21-00267-01
CIEhA8T5.zip	2CMV21-00267-01
CV.7z	2CMV21-00267-01
DJ.arj	2CMV21-00267-01
Document.rar	2CMV21-00267-01
El nuevo pedido esta en la lista..zip	2CMV21-00267-01
IMG_9787.zip	2CMV21-00267-01
Invoice Ref#17-01-2022.rar	2CMV21-00267-01
mail10929.pif	2CMV21-00267-01
message.pif	2CMV21-00267-01
New Oder 2022.gz	2CMV21-00267-01
pago.lzh	2CMV21-00267-01
PO#85012457.gz	2CMV21-00267-01
Purchase order docs. pdf.....zip	2CMV21-00267-01
Purchase Order.xlsx	2CMV21-00267-01
shipping documents.zip	2CMV21-00267-01
SWIFT007_010012022.r00	2CMV21-00267-01
SWIFT007_010012022.r15	2CMV21-00267-01
Tax Inv for Jan-2022 (FS).xlsx	2CMV21-00267-01
update status of order 07G050.r00	2CMV21-00267-01
XVS022-012022.xlsx	2CMV21-00267-01

Actualidad

Ciberconsejos para protegerse del ransomware

El ransomware es considerado una de las amenazas cibernéticas más importantes del último tiempo, ya que genera significativas pérdidas económicas y de seguridad para las empresas. El objetivo de este tipo de malware es secuestrar los datos de una organización y/o persona para posteriormente pedir un rescate.

Las pérdidas por ransomware se cuentan por varios cientos de millones de dólares anualmente. Purplesec, una firma norteamericana de ciberseguridad, estimó que el costo económico para las organizaciones víctimas de ransomware pasaron de $11,5 billones en 2019 a $20 billones este año 2020, aumentando el pago promedio por ataque en 104%. Solo en el área de la salud, el ransomware ha costado unos $157 millones de dólares. Para saber cómo protegerse y cómo actuar ante un malware, el CSIRT del Gobierno elaboró los siguientes consejos: https://www.csirt.gob.cl/recomendaciones/proteccion-del-ransomware/

Comando

El Comando de la Semana | No. 26 Hashcat

El Comando de la Semana hoy trae a Hashcat, herramienta que permite mejorar la seguridad de nuestros sistemas al analizar la fortaleza de las contraseñas utilizadas para ingresar a ellos.

Descarga el Comando de la Semana aquí: https://www.csirt.gob.cl/estadisticas/el-comando-de-la-semana-no-26/

Recomendaciones y buenas prácticas

- 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.

- Pablo Cyber Diver
- Rayen Castro
- Víctor Cofré
- Carolina Venegas
- Nelson Silva
- Pamela Palma
- Cristián Acuña
- Carol San Martin
- Carolina Cornejo
- Óscar Aguirre
- Óscar Guarda
- Kevin Anguita