10-06-2020 | Año 1 | N°49

# Boletín de Seguridad Cibernética

Semana del 04 al 11 de junio 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

**Parches**

**10**

**para vulnerabilidades**

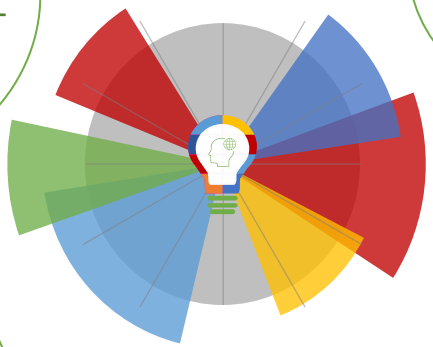
Las mitigaciones son útiles para productos de Mozilla, Talos Cisco, Grafana, Django, Microsft, Docker, Sony, Xen y LibreOffce.

**Se advirtieron**

**7**

**sitios fraudulentos**

Asociadas a 9 IP maliciosas



**Phishing**

**9**

**campañas**

Entre ellos se cuentan phishing bancarios, de servicios de pago, beneficios estatales y correos corporativos.

**IPs**

**117**

**bloqueadas**

Listado de IPs que trataron de realizar escaneos de puertos, DDoS o infectar códigos maliciosos, entre otros.

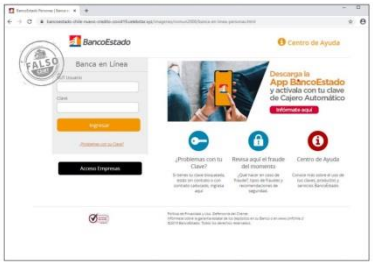
*Los datos recopilados corresponden a información publicada en diferentes secciones del sitio web https://www.csirt.gob.cl

# Contenido

Sitios fraudulentos ..... 3
Phishing ..... 7
Vulnerabilidades ..... 12
Indicadores de Compromisos ..... 19
Recomendaciones y Buenas Prácticas ..... 21
Investigación ..... 22
Muro de la Fama ..... 23

# Sitios fraudulentos

Imagen del sitio



| CSIRT advierte de sitio bancario fraudulento | |
|---|---|
| Alerta de seguridad cibernética | 8FFR20-00439-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Falsificación de Registros o Identidad |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 05 de Junio de 2020 |
| Última revisión | 05 de Junio de 2020 |
| **Indicadores de compromiso** | |
| URL | |
| hxxps://bancoestado-chile-nuevo-credito-covid19.celebstar[.]xyz/imagenes/comun2008/banca-en-linea-personas.html | |
| IP | |
| 94.237.77.204 | |
| **Enlaces para revisar el informe:** | |
| https://www.csirt.gob.cl/alertas/8ffr20-00439-01/ | |
| https://www.csirt.gob.cl/media/2020/06/8FFR20-00439-01.pdf | |

Imagen del sitio

| CSIRT advierte de portal bancario fraudulento | |
|---|---|
| Alerta de seguridad cibernética | 8FFR20-00440-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Falsificación de Registros o Identidad |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 05 de Junio de 2020 |
| Última revisión | 05 de Junio de 2020 |
| **Indicadores de compromiso** | |
| URL | |
| hxxp://www.ban.estado-creditos[.]net | |
| IP | |
| 85.187.132.184 | |
| **Enlaces para revisar el informe:** | |
| https://www.csirt.gob.cl/alertas/8ffr20-00440-01/ | |
| https://www.csirt.gob.cl/media/2020/06/8FFR20-00440-01.pdf | |

Imagen del sitio

| CSIRT advierte de sitio bancario fraudulento | |
|---|---|
| Alerta de seguridad cibernética | 8FFR20-00441-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Falsificación de Registros o Identidad |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 08 de Junio de 2020 |
| Última revisión | 08 de Junio de 2020 |
| **Indicadores de compromiso** | |
| URL | |
| banckaestada[.]info | |
| http[:]//banckaestada[.]info/1591634436/imagenes/comun2008/banca-en-linea-personas[.]html | |
| IP | |
| 139[.]59[.]25[.]203 | |
| **Enlaces para revisar el informe:** | |
| https://www.csirt.gob.cl/alertas/8ffr20-00441-01/ | |
| https://www.csirt.gob.cl/media/2020/06/8FFR20-00441-01.pdf | |

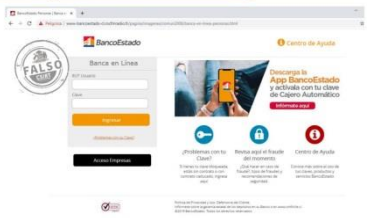
Imágenes del sitio

| CSIRT advierte de dos sitios bancarios para fraudes | |
|---|---|
| Alerta de seguridad cibernética | 8FFR20-00442-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Falsificación de Registros o Identidad |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 08 de Junio de 2020 |
| Última revisión | 08 de Junio de 2020 |
| **Indicadores de compromiso** | |
| URL | |
| bancoestsdo[.]cl | |
| https[:]//www.bancoestado.cl.personas.banca.en.linea.siyps[.]club/wpt/ | |
| IP | |
| 80[.]211[.]153[.]194 | |
| 54[.]153[.]28[.]78 | |
| **Enlaces para revisar el informe:** | |
| https://www.csirt.gob.cl/alertas/8ffr20-00442-01/ | |
| https://www.csirt.gob.cl/media/2020/06/8FFR20-00442-01.pdf | |

Imágenes del sitio

| CSIRT advierte de un sitio bancario fraudulento | |
|---|---|
| Alerta de seguridad cibernética | 8FFR20-00443-01 |
| 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 2020 |
| Última revisión | 09 de Junio de 2020 |
| **Indicadores de compromiso** | |
| URL | |
| https[:]//www.bancoestado.cl.personas.banca.en.linea.suzyxs[.]online/wpt/ | |
| IP | |
| 54[.]153[.]28[.]78 | |
| **Enlaces para revisar el informe:** | |
| https://www.csirt.gob.cl/alertas/8ffr20-00443-01/ | |
| https://www.csirt.gob.cl/media/2020/06/8FFR20-00443-01.pdf | |

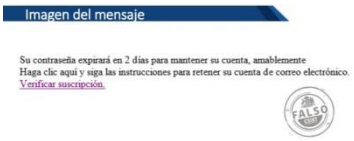
Imagen del sitio



| CSIRT advierte de portal bancario fraudulento | |
|---|---|
| Alerta de seguridad cibernética | 8FFR20-00444-01 |
| 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 2020 |
| Última revisión | 10 de Junio de 2020 |
| **Indicadores de compromiso** | |
| URL | |
| hxxps://www-bancoestado-cl.rocfmradio[.]fr/pagina/imagenes/comun2008/banca-en-linea-personas.html | |
| IP | |
| 193.26.21.0/24 | |
| **Enlaces para revisar el informe:** | |
| https://www.csirt.gob.cl/alertas/8ffr20-00444-01/ | |
| https://www.csirt.gob.cl/media/2020/06/8FFR20-00444-01.pdf | |


| CSIRT informa sobre un sitio bancario fraudulento | |
|---|---|
| Alerta de seguridad cibernética | 8FFR20-00445-01 |
| 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 2020 |
| Última revisión | 10 de Junio de 2020 |
| **Indicadores de compromiso** | |
| URL | |
| hxxp://www.credito-personal-bancoestado-chile.laurasunshine[.]online/imagenes/comun2008/banca-en-linea-personas.html | |
| IP | |
| 94.237.64.0/19 | |
| **Enlaces para revisar el informe:** | |
| https://www.csirt.gob.cl/alertas/8ffr20-00445-01/ | |
| https://www.csirt.gob.cl/media/2020/06/8FFR20-00445-01.pdf | |

# Phishing




| CSIRT advierte de phihsing por expiración de contraseña | |
|---|---|
| Alerta de seguridad cibernética | 8FPH20-00237-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Phishing |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 03 de Junio de 2020 |
| Última revisión | 03 de Junio de 2020 |
| **Indicadores de compromiso** | |
| URL | |
| hxxps://zmbr-278921.rj.r.appspot[.]com/zim.html?correo.zimbra.com | |
| **Enlaces para revisar el informe:** | |
| https://www.csirt.gob.cl/alertas/8fph20-00237-01/ | |
| https://www.csirt.gob.cl/media/2020/06/8FPH20-00237-01.pdf | |


| CSIRT advierte de phishing por sincronización de dispositivo bancario | |
|---|---|
| Alerta de seguridad cibernética | 8FPH20-00238-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Phishing |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 03 de Junio de 2020 |
| Última revisión | 03 de Junio de 2020 |
| **Indicadores de compromiso** | |
| URL | |
| hxxps://www.ausy[.]fr/c47d86e082d49717f5ba58476dd5d34d | |
| hxxps://scotiportalenlinea-cl[.]com/ | |
| IP | |
| [212.24.111.24] | |
| [194.135.88.52] | |
| [185.5.54.34] | |
| [195.181.242.207] | |
| [194.135.84.68] | |
| [195.181.244.195] | |
| [212.24.99.29] | |
| Otros IOCs del informe: | |
| 7 sender | |
| **Enlaces para revisar el informe:** | |
| https://www.csirt.gob.cl/alertas/8fph20-00238-01/ | |
| https://www.csirt.gob.cl/media/2020/06/8FPH20-00238-01.pdf | |

Imagen del mensaje


| CSIRT advierte campaña de phishing por abono de beneficio | |
|---|---|
| Alerta de seguridad cibernética | 8FPH20-00239-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Phishing |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 04 de Junio de 2020 |
| Última revisión | 04 de Junio de 2020 |
| **Indicadores de compromiso** | |
| URL | |
| hxxp://bigforum[.]in/js/enviar.php?l=805038886 | |
| hxxps://touroholic[.]com/Pension/www.bancoestado.cl/ | |
| IP | |
| [45.236.130.86] | |
| [27.54.133.65] | |
| Otros IOCs del informe: | |
| 2 sender | |
| **Enlaces para revisar el informe:** | |
| https://www.csirt.gob.cl/alertas/8fph20-00239-01/ | |
| https://www.csirt.gob.cl/media/2020/06/8FPH20-00239-01.pdf | |

Imagen del mensaje


| CSIRT advierte de phishing bancario por bloqueo de cuenta | |
|---|---|
| Alerta de seguridad cibernética | 8FPH20-00240-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Phishing |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 05 de Junio de 2020 |
| Última revisión | 05 de Junio de 2020 |
| **Indicadores de compromiso** | |
| URL | |
| hxxp://talcaweb[.]com/Activacion/cuenta-pkwn/ | |
| hxxp://rekuteku[.]com/load/imagenes/comun2008/banca-en-linea-personas.html | |
| IP | |
| [45.7.231.109] | |
| Otros IOCs del informe: | |
| 1 sender | |
| **Enlaces para revisar el informe:** | |
| https://www.csirt.gob.cl/alertas/8fph20-00240-01/ | |
| https://www.csirt.gob.cl/media/2020/06/8FPH20-00240-01.pdf | |

Imagen del mensaje


| CSIRT advierte phishing bancario por abono de pensión | |
|---|---|
| Alerta de seguridad cibernética | 8FPH20-00241-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Phishing |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 05 de Junio de 2020 |
| Última revisión | 05 de Junio de 2020 |
| **Indicadores de compromiso** | |
| URL | |
| hxxp://bigforum[.]in/js/enviar.php?l=805038886 | |
| hxxps://bit[.]ly/3eMdIBf?l=www.bancoestado.cl | |
| hxxps://petya.terytoriakrasy[.]com.ua/activacion/cuenta-zdgw/ | |
| hxxps://mechri-ts[.]com/Pension/www.bancoestado.cl/pagina/imagenes/comun2008/banca-en-linea-personas.html | |
| IP | |
| [45.236.130.86] | |
| Otros IOCs del informe: | |
| 1 sender | |
| **Enlaces para revisar el informe:** | |
| https://www.csirt.gob.cl/alertas/8fph20-00241-01/ | |
| https://www.csirt.gob.cl/media/2020/06/8FPH20-00241-01.pdf | |

Imagen del mensaje


| CSIRT advierte phishing bancario por abono de beneficio estatal | |
|---|---|
| Alerta de seguridad cibernética | 8FPH20-00242-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Phishing |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 10 de Junio de 2020 |
| Última revisión | 10 de Junio de 2020 |
| **Indicadores de compromiso** | |
| URL | |
| hxxp://bigforum[.]in/js/enviar.php?l=805038886 | |
| hxxps://bit[.]ly/3eMdIBf?l=www.bancoestado.cl | |
| hxxps://petya.terytoriakrasy[.]com.ua/activacion/cuenta-zdgw/ | |
| hxxps://www-bancoestado-cl.rocfmradio.fr/pagina/imagenes/comun2008/banca-en-linea-personas.html | |
| IP | |
| [91.221.70.106] | |
| Otros IOCs del informe: | |
| 1 sender | |
| **Enlaces para revisar el informe:** | |
| https://www.csirt.gob.cl/alertas/8fph20-00242-01/ | |
| https://www.csirt.gob.cl/media/2020/06/8FPH20-00242-01.pdf | |

Imagen del mensaje


| CSIRT advierte phishing por falsa compensación en estafa internacional | |
|---|---|
| Alerta de seguridad cibernética | 8FPH20-00243-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Phishing |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 10 de Junio de 2020 |
| Última revisión | 10 de Junio de 2020 |
| **Indicadores de compromiso** | |
| IP | |
| [91.221.70.106] | |
| Otros IOCs del informe: | |
| 1 sender | |
| **Enlaces para revisar el informe:** | |
| https://www.csirt.gob.cl/alertas/8fph20-00243-01/ | |
| https://www.csirt.gob.cl/media/2020/06/8FPH20-00243-01.pdf | |

Imagen del mensaje


| CSIRT advierte phishing por caducidad de tarjeta de coordenadas | |
|---|---|
| Alerta de seguridad cibernética | 8FPH20-00244-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Phishing |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 11 de Junio de 2020 |
| Última revisión | 11 de Junio de 2020 |
| **Indicadores de compromiso** | |
| URL | |
| hxxps://bit[.]ly/2XQgvE8 | |
| hxxp://cifras[.]cl/es/ | |
| http://bancamovilseguro.tonohost.com/imagenes/comun2008/banca-en-linea-personas.html | |
| **Enlaces para revisar el informe:** | |
| https://www.csirt.gob.cl/alertas/8fph20-00244-01/ | |
| https://www.csirt.gob.cl/media/2020/06/8FPH20-00244-01.pdf | |


| CSIRT advierte smishing que ofrece hielera de cerveza | |
|---|---|
| Alerta de seguridad cibernética | 8FPH20-00245-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Phishing |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 11 de Junio de 2020 |
| Última revisión | 11 de Junio de 2020 |
| **Indicadores de compromiso** | |
| URL | |
| hxxps://heineken.regalo[.]top/ | |
| IP | |
| [91.221.70.106] | |
| **Enlaces para revisar el informe:** | |
| https://www.csirt.gob.cl/alertas/8fph20-00245-01/ | |
| https://www.csirt.gob.cl/media/2020/06/8FPH20-00245-01.pdf | |

# Vulnerabilidades


| CSIRT comparte actualizaciones de Mozilla para Thunderbird | |
|---|---|
| Alerta de seguridad cibernética | 9VSA20-00234-01 |
| Clase de alerta | Vulnerabilidad |
| Tipo de incidente | Sistema y/o Software Abierto |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 04 de Junio de 2020 |
| Última revisión | 04 de Junio de 2020 |
| **CVE** | |
| CVE-2020-12399 -CVE-2020-12405 -CVE-2020-12406, CVE-2020-12410 -CVE-2020-12398 | |
| **Fabricante** | |
| Mozilla | |
| **Producto afectado** | |
| Mozilla Thunderbird entre las versiones 60.0 y 68.8.1. | |
| **Enlaces para revisar el informe:** | |
| https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00234-01/ | |
| https://www.csirt.gob.cl/media/2020/06/9VSA20-00234-01.pdf | |


| CSIRT comparte actualizaciones de Talos Cisco para Zoom | |
|---|---|
| Alerta de seguridad cibernética | 9VSA20-00235-01 |
| Clase de alerta | Vulnerabilidad |
| Tipo de incidente | Sistema y/o Software Abierto |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 05 de Junio de 2020 |
| Última revisión | 05 de Junio de 2020 |
| **CVE** | |
| CVE-2020-6109 -CVE-2020-6110 | |
| **Fabricante** | |
| Talos Cisco | |
| **Producto afectado** | |
| Actualizar a la versión 4.6.12 de Zoom. | |
| **Enlaces para revisar el informe:** | |
| https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00235-01/ | |
| https://www.csirt.gob.cl/media/2020/06/9VSA20-00235-01.pdf | |


| CSIRT comparte actualizaciones liberadas por FortiNet | |
|---|---|
| Alerta de seguridad cibernética | 9VSA20-00236-01 |
| Clase de alerta | Vulnerabilidad |
| Tipo de incidente | Sistema y/o Software Abierto |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 06 de Junio de 2020 |
| Última revisión | 06 de Junio de 2020 |
| **CVE** | |
| FG-IR-19-306 -CVE-2018-13367 -CVE-2019-16150 CVE-2020-9292 -CVE-2020-6640 | |
| **Fabricante** | |
| Fortinet | |
| **Producto afectado** | |
| FortiGateCloud versión 4.4. | |
| **Enlaces para revisar el informe:** | |
| https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00236-01/ | |
| https://www.csirt.gob.cl/media/2020/06/9VSA20-00236-01.pdf | |


| CSIRT comparte actualizaciones obtenidas de Grafana | |
|---|---|
| Alerta de seguridad cibernética | 9VSA20-00237-01 |
| Clase de alerta | Vulnerabilidad |
| Tipo de incidente | Sistema y/o Software Abierto |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 06 de Junio de 2020 |
| Última revisión | 06 de Junio de 2020 |
| **CVE** | |
| CVE-2020-13379 | |
| **Fabricante** | |
| Grafana | |
| **Productos afectados** | |
| Grafana desde la versión 3.0.1 hasta la versión 7.0.1. | |
| **Enlaces para revisar el informe:** | |
| https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00237-01/ | |
| https://www.csirt.gob.cl/media/2020/06/9VSA20-00237-01.pdf | |


| CSIRT comparte actualizaciones liberadas por Docker | |
|---|---|
| Alerta de seguridad cibernética | 9VSA20-00238-01 |
| Clase de alerta | Vulnerabilidad |
| Tipo de incidente | Sistema y/o Software Abierto |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 08 de Junio de 2020 |
| Última revisión | 08 de Junio de 2020 |
| **CVE** | |
| CVE-2020-13401 | |
| **Fabricante** | |
| Docker | |
| **Producto afectado** | |
| Docker desde la versión 19.03.0 hasta la versión 19.03.10. | |
| **Enlaces para revisar el informe:** | |
| https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00238-01/ | |
| https://www.csirt.gob.cl/media/2020/06/9VSA20-00238-01.pdf | |


| CSIRT comparte vulnerabilidad y mitigación para múltiples audífonos libres de Sony | |
|---|---|
| Alerta de seguridad cibernética | 9VSA20-00239-01 |
| Clase de alerta | Vulnerabilidad |
| Tipo de incidente | Sistema y/o Software Abierto |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 08 de Junio de 2020 |
| Última revisión | 08 de Junio de 2020 |
| **CVE** | |
| CVE-2020-5589 | |
| **Fabricante** | |
| Sony | |
| **Producto afectado** | |
| Múltiples audífonos libres de Sony. | |
| **Enlaces para revisar el informe:** | |
| https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00239-01/ | |
| https://www.csirt.gob.cl/media/2020/06/9VSA20-00239-01.pdf | |


| CSIRT comparte actualizaciones para LibreOffice | |
|---|---|
| Alerta de seguridad cibernética | 9VSA20-00240-01 |
| Clase de alerta | Vulnerabilidad |
| Tipo de incidente | Sistema y/o Software Abierto |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 09 de Junio de 2020 |
| Última revisión | 09 de Junio de 2020 |
| **CVE** | |
| CVE-2020-12802 -CVE-2020-12803 | |
| **Fabricante** | |
| LibreOffice | |
| **Producto afectado** | |
| LibreOffice versión 6.4.3 y anteriores. | |
| **Enlaces para revisar el informe:** | |
| https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00240-01/ | |
| https://www.csirt.gob.cl/media/2020/06/9VSA20-00240-01.pdf | |


| CSIRT comparte actualizaciones liberadas por Microsoft | |
|---|---|
| Alerta de seguridad cibernética | 9VSA20-00241-01 |
| 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 2020 |
| Última revisión | 10 de Junio de 2020 |
| **CVE** | |
| ADV200010 , CVE-2020-1223 , CVE-2020-1295, CVE-2020-1181 , CVE-2020-1225 , CVE-2020-1296, CVE-2020-1148 , CVE-2020-1226 , CVE-2020-1297, CVE-2020-1160 , CVE-2020-1229 , CVE-2020-1298, CVE-2020-1163 , CVE-2020-1232 , CVE-2020-1301, CVE-2020-1170 , CVE-2020-1242 , CVE-2020-1315, CVE-2020-1177 , CVE-2020-1261 , CVE-2020-1318, CVE-2020-1178 , CVE-2020-1263 , CVE-2020-1320, CVE-2020-1183 , CVE-2020-1268 , CVE-2020-1321, CVE-2020-1206 , CVE-2020-1284 , CVE-2020-1322, CVE-2020-1217 , CVE-2020-1289 , CVE-2020-1323, CVE-2020-1220 , CVE-2020-1290 , CVE-2020-1329, CVE-2020-0915 , CVE-2020-1237 , CVE-2020-1281 CVE-2020-0916 , CVE-2020-1238 , CVE-2020-1282, CVE-2020-0986 , CVE-2020-1239 , CVE-2020-1283, CVE-2020-1073 , CVE-2020-1241 , CVE-2020-1286, CVE-2020-1120 , CVE-2020-1244 , CVE-2020-1287, CVE-2020-1162 , CVE-2020-1246 , CVE-2020-1291, CVE-2020-1194 , CVE-2020-1247 , CVE-2020-1292, CVE-2020-1195 , CVE-2020-1248 , CVE-2020-1293, CVE-2020-1196 , CVE-2020-1251 , CVE-2020-1294, CVE-2020-1197 , CVE-2020-1253 , CVE-2020-1299, CVE-2020-1199 , CVE-2020-1254 , CVE-2020-1300, CVE-2020-1201 , CVE-2020-1255 , CVE-2020-1302, CVE-2020-1202 , CVE-2020-1257 , CVE-2020-1304, CVE-2020-1203 , CVE-2020-1258 , CVE-2020-1305 CVE-2020-1204 , CVE-2020-1259 , CVE-2020-1306, CVE-2020-1207 , CVE-2020-1260 , CVE-2020-1307, CVE-2020-1208 , CVE-2020-1262 , CVE-2020-1309, CVE-2020-1209 , CVE-2020-1264 , CVE-2020-1310, CVE-2020-1211 , CVE-2020-1265 , CVE-2020-1311, CVE-2020-1212 , CVE-2020-1266 , CVE-2020-1312, CVE-2020-1213 , CVE-2020-1269 , CVE-2020-1313, CVE-2020- | |

| |
|---|
| 1214 , CVE-2020-1270 , CVE-2020-1314, CVE-2020-1215 , CVE-2020-1271 , CVE-2020-1316, CVE-2020-1216 , CVE-2020-1272 , CVE-2020-1317 CVE-2020-1219 , CVE-2020-1273 , CVE-2020-1324, CVE-2020-1222 , CVE-2020-1274 , CVE-2020-1327, CVE-2020-1230 , CVE-2020-1275 , CVE-2020-1331, CVE-2020-1231 , CVE-2020-1276 , CVE-2020-1334, CVE-2020-1233 , CVE-2020-1277 , CVE-2020-1340, CVE-2020-1234 , CVE-2020-1278 , CVE-2020-1343, CVE-2020-1235 , CVE-2020-1279 , CVE-2020-1348, CVE-2020-1236 , CVE-2020-1280 |
| **Fabricante** |
| Microsoft |
| **Productos afectados** |
| Adobe Flash Player (ADV200010)<br>Azure DevOps Server 2019<br>ChakraCore<br>Internet Explorer 9, 11<br>Microsoft 365 Apps for Enterprise (32-bit y 64-bit)<br>Microsoft Bing Search for Android<br>Microsoft Edge (Chromium-based, EdgeHTML-based)<br>Microsoft Excel<br>2010 Service Pack 2 (32-bit y 64-bit editions)<br>2013 RT Service Pack 1<br>2013 Service Pack 1 (32-bit y 64-bit editions)<br>2016 (32-bit y 64-bit editions)<br>Microsoft Forefront Endpoint Protection 2010<br>Microsoft Office<br>2010 Service Pack 2 (32-bit y 64-bit editions)<br>2013 RT Service Pack 1<br>2013 Service Pack 1 (32-bit y 64-bit editions)<br>2016 (32-bit y 64-bit editions)<br>2016 for Mac<br>2019 (32-bit y 64-bit editions)<br>2019 for Mac<br>Microsoft Project<br>2010 Service Pack 2 (32-bit y 64-bit editions)<br>2013 Service Pack 1 (32-bit y 64-bit editions)<br>2016 (32-bit y 64-bit editions)<br>Microsoft Security Essentials<br>Microsoft SharePoint<br>Enterprise Server 2013 Service Pack 1<br>Enterprise Server 2016<br>Foundation 2010 Service Pack 2<br>Foundation 2013 Service Pack 1<br>Server 2010 Service Pack 2<br>Server 2019<br>Microsoft System Center<br>2012 Endpoint Protection<br>2012 R2 Endpoint Protection<br>Endpoint Protection<br>Microsoft Visual Studio<br>2015 Update 3<br>2017 version 15.9 (incluidos 15.1 – 15.8) |

| |
|---|
| 2019 version 16.0<br>2019 version 16.4 (incluidos 16.0 – 16.3)<br>2019 version 16.6 (incluidos 16.0 – 16.5)<br>Code Live Share extension<br>Microsoft Word<br>2010 Service Pack 2 (32-bit y 64-bit editions)<br>2013 RT Service Pack 1<br>2013 Service Pack 1 (32-bit y 64-bit editions)<br>2016 (32-bit y 64-bit editions)<br>Word para Android<br>NuGetGallery<br>System Center 2016 Operations Manager<br>Windows 10<br>Version 1607, 1709, 1803, 1809, 1903, 1909, 2004, para 32 y 64 bit<br>Windows 7<br>32-bit Systems Service Pack 1<br>x64-based Systems Service Pack 1<br>Windows 8.1<br>32-bit systems<br>x64-based systems<br>Windows Defender<br>Windows RT 8.1<br>Windows Server 2008<br>32-bit Systems Service Pack 2<br>32-bit Systems Service Pack 2 (Server Core installation)<br>Itanium-Based Systems Service Pack 2<br>x64-based Systems Service Pack 2<br>x64-based Systems Service Pack 2 (Server Core installation)<br>R2 for Itanium-Based Systems Service Pack 1<br>R2 for x64-based Systems Service Pack 1<br>R2 for x64-based Systems Service Pack 1 (Server Core installation)<br>Windows Server 2012<br>2012<br>Server Core installation<br>R2 y R2 (Server Core installation)<br>Windows Server 2016<br>2016<br>Server Core installation<br>Windows Server 2019<br>2019<br>Server Core installation<br>Windows Server<br>version 1803 (Server Core Installation)<br>version 1903 (Server Core installation)<br>version 1909 (Server Core installation)<br>version 2004 (Server Core installation) |
| **Enlaces para revisar el informe:** |
| https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00241-01/ |
| https://www.csirt.gob.cl/media/2020/06/9VSA20-00241-01.pdf |


| CSIRT comparte vulnerabilidad y mitigación liberada por Django para desarrollo web | |
|---|---|
| Alerta de seguridad cibernética | 9VSA20-00242-01 |
| Clase de alerta | Vulnerabilidad |
| Tipo de incidente | Sistema y/o Software Abierto |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 11 de Junio de 2020 |
| Última revisión | 11 de Junio de 2020 |
| **CVE** | |
| CVE-2020-13254 -CVE-2020-13596 | |
| **Fabricante** | |
| Django | |
| **Producto afectado** | |
| Django rama maestra.<br>Django versión 3.1 (En estado alpha).<br>Django versión 3.0.<br>Django versión 2.2. | |
| **Enlaces para revisar el informe:** | |
| https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00242-01/ | |
| https://www.csirt.gob.cl/media/2020/06/9VSA20-00242-01.pdf | |


| CSIRT comparte vulnerabilidad y mitigación liberada por Xen | |
|---|---|
| Alerta de seguridad cibernética | 9VSA20-00243-01 |
| Clase de alerta | Vulnerabilidad |
| Tipo de incidente | Sistema y/o Software Abierto |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 11 de Junio de 2020 |
| Última revisión | 11 de Junio de 2020 |
| **CVE** | |
| CVE-2020-0543 | |
| **Fabricante** | |
| Xen | |
| **Producto afectado** | |
| Todos los sistemas con arquitectura x86 de Intel que utilicen Xen son vulnerables.<br>No se ha comprobado que otras arquitecturas y otros procesadores (como ADM) sean vulnerables. | |
| **Enlaces para revisar el informe:** | |
| https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00243-01/ | |
| https://www.csirt.gob.cl/media/2020/06/9VSA20-00243-01.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:

| IoC | Motivo | IoC | Motivo |
|---|---|---|---|
| 193.169.252.21 | Port Scan | 51.222.38.12 | Port Scan |
| 77.247.108.2 | Port Scan | 51.222.38.10 | Port Scan |
| 52.130.83.171 | Port Scan | 51.222.38.3 | Port Scan |
| 94.111.43.1 | Port Scan | 51.222.38.11 | Port Scan |
| 37.49.230.81 | Port Scan | 51.222.38.14 | Port Scan |
| 104.244.72.51 | Port Scan | 173.237.17.68 | Port Scan |
| 185.200.118.49 | Port Scan | 85.143.218.203 | Malware |
| 128.14.180.110 | Port Scan | 74.141.90.30 | Port Scan |
| 139.162.216.32 | Malware | 185.166.153.98 | Port Scan |
| 190.114.244.182 | Malware | 185.39.11.38 | Port Scan |
| 46.101.196.229 | Port Scan | 185.39.11.47 | Port Scan |
| 159.89.224.99 | Port Scan | 185.39.11.57 | Port Scan |
| 156.96.117.151 | Port Scan | 185.39.11.55 | Port Scan |
| 159.89.157.126 | Port Scan | 185.39.11.39 | Port Scan |
| 128.14.180.110 | Port Scan | 139.59.90.0 | Port Scan |
| 109.236.60.34 | Port Scan | 103.145.12.54 | Port Scan |
| 62.122.136.241 | Port Scan | 167.172.100.75 | Port Scan |
| 62.122.136.242 | Port Scan | 103.82.210.12 | Port Scan |
| 157.52.193.83 | Port Scan | 190.44.232.173 | DDoS |
| 157.52.193.77 | Port Scan | 74.82.47.42 | Port Scan |
| 83.97.20.149 | Port Scan | 74.82.47.62 | Port Scan |
| 192.241.230.228 | Port Scan | 74.82.47.58 | Port Scan |
| 159.89.237.165 | Port Scan | 74.82.47.16 | Port Scan |
| 195.154.189.23 | Port Scan | 74.82.47.60 | Port Scan |
| 157.7.138.240 | Port Scan | 92.118.160.17 | Port Scan |
| 103.145.12.153 | Port Scan | 94.130.16.50 | Port Scan |
| 172.255.251.212 | Port Scan | 184.105.139.90 | Port Scan |
| 167.99.96.248 | DDoS | 92.118.161.57 | Port Scan |
| 178.62.54.247 | Port Scan | 46.105.117.221 | Port Scan |
| 163.172.8.227 | Port Scan | 51.91.190.40 | Port Scan |

| | | | |
|---|---|---|---|
| 185.53.88.231 | Port Scan | 176.31.146.22 | Port Scan |
| 89.144.47.243 | Port Scan | 45.143.220.151 | Port Scan |
| 87.98.219.59 | Port Scan | 185.53.88.247 | Port Scan |
| 185.200.118.66 | Port Scan | 163.18.68.78 | Port Scan |
| 185.122.200.160 | Port Scan | 128.199.182.244 | Port Scan |
| 62.171.171.32 | Port Scan | 83.97.20.224 | Port Scan |
| 79.124.62.18 | Port Scan | 199.201.110.206 | Port Scan |
| 134.73.232.201 | Port Scan | 185.200.34.176 | Port Scan |
| 188.166.153.212 | Port Scan | 92.118.161.41 | Port Scan |
| 185.53.88.188 | Port Scan | 185.165.190.34 | Port Scan |
| 103.145.12.145 | Port Scan | 51.255.109.165 | Port Scan |
| 162.243.136.27 | Port Scan | 216.180.117.187 | Port Scan |
| 162.243.198.189 | Port Scan | 23.94.150.234 | Port Scan |
| 206.189.90.210 | Port Scan | 193.37.255.114 | Port Scan |
| 192.241.209.175 | Port Scan | 220.124.130.66 | Port Scan |
| 185.97.32.6 | Malware | 1.246.223.3 | Port Scan |
| 36.89.106.69 | Malware | 125.212.217.214 | Port Scan |
| 51.222.38.7 | Port Scan | 51.255.109.169 | Port Scan |
| 51.222.38.8 | Port Scan | 109.64.124.251 | Port Scan |
| 51.222.38.0 | Port Scan | 92.118.161.25 | Port Scan |
| 51.222.38.15 | Port Scan | 43.245.222.163 | Port Scan |
| 51.222.38.5 | Port Scan | 1.246.223.58 | Port Scan |
| 51.222.38.13 | Port Scan | 51.255.109.161 | Port Scan |
| 51.222.38.9 | Port Scan | 103.145.12.129 | Port Scan |
| 51.222.38.4 | Port Scan | 77.247.110.6 | Port Scan |
| 51.222.38.2 | Port Scan | 45.143.220.233 | Port Scan |
| 51.222.38.1 | Port Scan | 103.117.172.206 | Malware |
| 51.222.38.6 | Port Scan | 105.209.235.113 | Malware |
| 159.65.163.234 | Port Scan | | |

# Recomendaciones y Buenas Prácticas

## Recomendaciones generales de seguridad

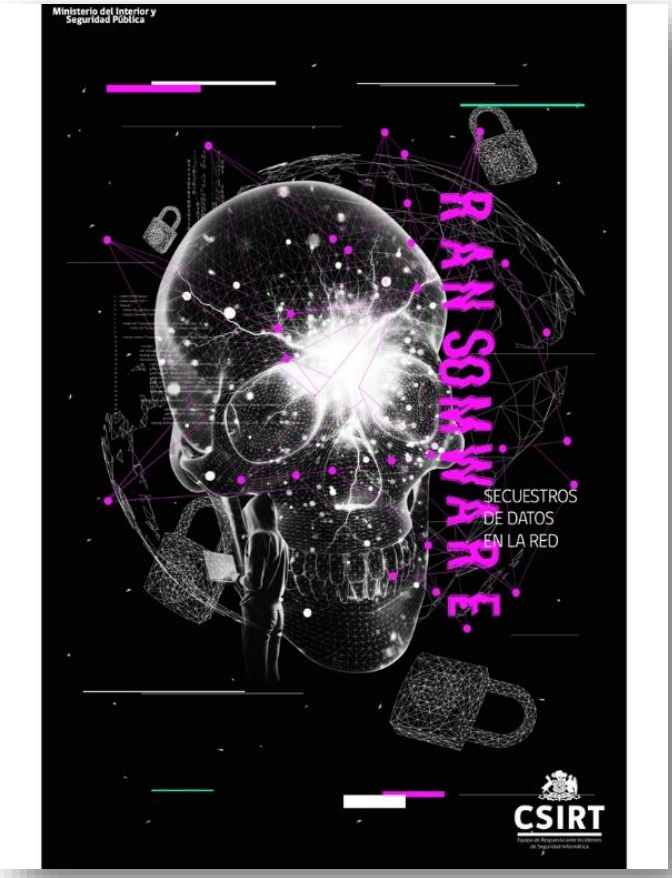
- No abrir correos ni mensajes de dudosa procedencia.
- Desconfiar de los enlaces y archivos en los mensajes o correo.
- Mantener actualizadas sus plataformas (Office, Windows, Adobe Acrobat, Oracle Java y otras).
- Ser escépticos frente ofertas, promociones o premios increíbles que se ofrecen por internet
- 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.

# Investigación

## Ransomware. Secuestro de datos en la red

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la séptima edición de su publicación sobre amenazas cibernéticas el que analiza la amenaza del Ransomware. Este artículo que fue elaborado por Carlos Silva Caffi junto con Hernán Espinoza Medina, ambos analistas de nivel 2 de CSIRT.

El ransomware es un malware con la capacidad de cifrar archivos en una computadora o sistemas informáticos completos, y posee una clave para descifrar la data. Su objetivo es secuestrar información hasta que la víctima pague un rescate, el que normalmente se debe pagar en criptomonedas. Este tipo malware es un gran negocio para los atacantes, y es responsable de cientos de millones de dólares en pérdidas anualmente. Debido a la gran cantidad de dinero que se gana, las nuevas versiones aparecen con frecuencia y la evidencia respalda la idea de que es una amenaza en constante crecimiento.




**Ver en:** https://www.csirt.gob.cl/reportes/an2-2020-07/

# 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.

- Matia Cornejo
  Linkedin:
  https://www.linkedin.com/in/matia-cornejo/
- Romel Rivas
  Linkedin:
  https://www.linkedin.com/in/romelrivas/
- Mauricio Cabrales
  Linkedin:
  https://www.linkedin.com/in/mauricio-cabrales-3224a244/

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2020.06.13 12:20:25 -04'00'