12-01-2020 | Año 2 | N°71

# Boletín de Seguridad Cibernética

Semana del 05 al 11 de Noviembre 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

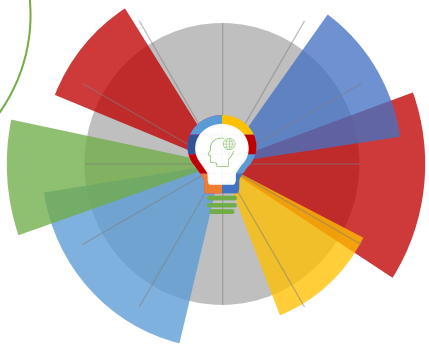
# Resumen de la semana en cifras

**Hash**

**10**

**Sha 256**

Asociadas a múltiples campañas de phishing son archivos que contienen malware



**Se advirtieron**

**8**

**URLs**

Asociadas a sitios fraudulentos y múltiples campañas de phishing y malware

**Parches**

**118**

**para vulnerabilidades**

Las mitigaciones son útiles para productos Windows, Chrome, WhatsApp y Samba.

**IPs**

**20**

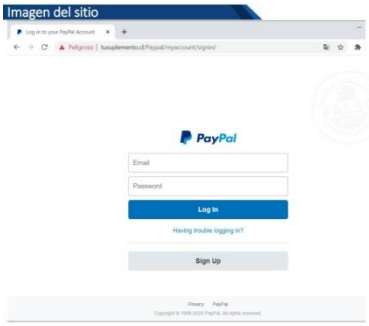
**Informadas**

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



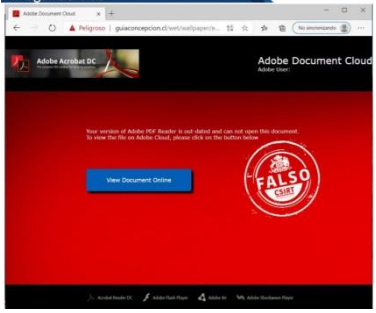

| CSIRT advierte de suplantación de sitio de pagos en línea | |
|---|---|
| Alerta de seguridad cibernética | 8FFR20-00820-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Falsificación de Registros o Identidad |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 07 de Noviembre de 2020 |
| Última revisión | 07 de Noviembre de 2020 |
| **Indicadores de compromiso** | |
| URL | |
| http[:]//www.tusuplemento[.]cl/Paypal/myaccount/signin/ | |
| IP | |
| [198.57.244.93] | |
| **Enlaces para revisar el informe:** | |
| https://www.csirt.gob.cl/alertas/8ffr20-00820-01/ | |
| https://www.csirt.gob.cl/media/2020/11/8FFR20-00820-01.pdf | |


| CSIRT advierte de portal que suplanta a web de banco | |
|---|---|
| Alerta de seguridad cibernética | 8FFR20-00821-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Falsificación de Registros o Identidad |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 07 de Noviembre de 2020 |
| Última revisión | 07 de Noviembre de 2020 |
| **Indicadores de compromiso** | |
| URL | |
| https[:]//sconsumer.e-pagos[.]cl/eftPP/ | |
| IP | |
| 200[.]75[.]7[.]241 | |
| **Enlaces para revisar el informe:** | |
| https://www.csirt.gob.cl/alertas/8ffr20-00821-01/ | |
| https://www.csirt.gob.cl/media/2020/11/8FFR20-00821-01.pdf | |


| CSIRT advierte de web que suplanta servicio de alojamiento de archivos | |
|---|---|
| Alerta de seguridad cibernética | 8FFR20-00822-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Falsificación de Registros o Identidad |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 07 de Noviembre de 2020 |
| Última revisión | 07 de Noviembre de 2020 |
| **Indicadores de compromiso** | |
| URL | |
| https://www.ecotimes.cl/office/365/ | |
| IP | |
| 45[.]239[.]108[.]252 | |
| **Enlaces para revisar el informe:** | |
| https://www.csirt.gob.cl/alertas/8ffr20-00822-01/ | |
| https://www.csirt.gob.cl/media/2020/11/8FFR20-00822-01.pdf | |

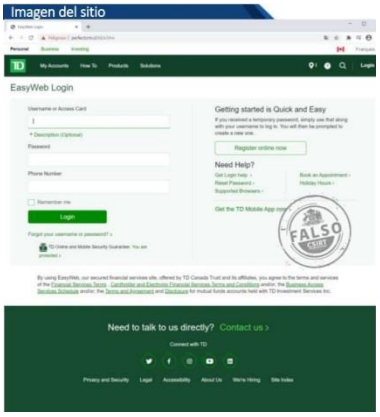

| CSIRT advierte de sitio que suplanta a web de banco | |
|---|---|
| Alerta de seguridad cibernética | 8FFR20-00823-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Falsificación de Registros o Identidad |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 07 de Noviembre de 2020 |
| Última revisión | 07 de Noviembre de 2020 |
| **Indicadores de compromiso** | |
| URL | |
| http[:]//zax-associates[.]com/www.bancoestado.cl/pagina/imagenes/comun2008/banca-en-linea-personas.html | |
| IP | |
| 91[.]220[.]196[.]45 | |
| **Enlaces para revisar el informe:** | |
| https://www.csirt.gob.cl/alertas/8ffr20-00823-01/ | |
| https://www.csirt.gob.cl/media/2020/11/8FFR20-00823-01.pdf | |

Imagen del sitio




| CSIRT advierte de sitio que suplanta a sitio de plataforma de software | |
|---|---|
| Alerta de seguridad cibernética | 8FFR20-00824-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Falsificación de Registros o Identidad |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 10 de Noviembre de 2020 |
| Última revisión | 10 de Noviembre de 2020 |
| **Indicadores de compromiso** | |
| URL | |
| http[:]//guiaconcepcion[.]cl/wet/wallpaper/error.php | |
| IP | |
| [162.241.89.50] | |
| **Enlaces para revisar el informe:** | |
| https://www.csirt.gob.cl/alertas/8ffr20-00824-01/ | |
| https://www.csirt.gob.cl/media/2020/11/8FFR20-00824-01.pdf | |

Imagen del sitio




| CSIRT advierte sitio bancario falso | |
|---|---|
| Alerta de seguridad cibernética | 8FFR20-00825-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Falsificación de Registros o Identidad |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 11 de Noviembre de 2020 |
| Última revisión | 11 de Noviembre de 2020 |
| **Indicadores de compromiso** | |
| URL | |
| http[:]//perfectcrm[.]cl/td/e.htm | |
| IP | |
| [201.148.107.69] | |
| **Enlaces para revisar el informe:** | |
| https://www.csirt.gob.cl/alertas/8ffr20-00825-01/ | |
| https://www.csirt.gob.cl/media/2020/11/8FFR20-00825-01-1.pdf | |

# Phishing

Imagen del mensaje


| CSIRT advierte de phishing bancario por supuesta caducidad de clave | |
|---|---|
| Alerta de seguridad cibernética | 8FPH20-00325-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Phishing |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 09 de Noviembre de 2020 |
| Última revisión | 09 de Noviembre de 2020 |
| **Indicadores de compromiso** | |
| URL | |
| http[:]//mariap.webd[.]pl/_personas/centro-de-ayuda/ | |
| http[:]//asedl[.]am/Suppor/pagina/imagenes/comun2008/banca-en-linea-personas.html | |
| IP | |
| [45.7.231.17] | |
| **Enlaces para revisar el informe:** | |
| https://www.csirt.gob.cl/alertas/8fph20-00325-01/ | |
| https://www.csirt.gob.cl/media/2020/11/8FPH20-00325-01.pdf | |

# Vulnerabilidades


| CSIRT comparte actualizaciones obtenidas de Mozilla | |
|---|---|
| Alerta de seguridad cibernética | 9VSA20-00317-01 |
| Clase de alerta | Vulnerabilidad |
| Tipo de incidente | Sistema y/o Software Abierto |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 05 de Noviembre de 2020 |
| Última revisión | 05 de Noviembre de 2020 |
| **CVE** | |
| CVE-2020-15679 | |
| **Fabricante** | |
| Mozilla | |
| **Productos afectados** | |
| Mozilla VPN para Android versión 1.1.0.<br>Mozilla VPN para Windows versiones anteriores a la 1.2.2.<br>Mozilla VPN para iOS versión 1.0.7 | |
| **Enlaces para revisar el informe:** | |
| https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00317-01/ | |
| https://www.csirt.gob.cl/media/2020/11/9VSA20-00317-01.pdf | |


| CSIRT comparte actualizaciones obtenidas de Wireshark | |
|---|---|
| Alerta de seguridad cibernética | 9VSA20-00318-01 |
| Clase de alerta | Vulnerabilidad |
| Tipo de incidente | Sistema y/o Software Abierto |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 05 de Noviembre de 2020 |
| Última revisión | 05 de Noviembre de 2020 |
| **CVE** | |
| CVE-2020-25862 - CVE-2020-25863 - CVE-2020-25866 | |
| **Fabricante** | |
| Wireshark | |
| **Productos afectados** | |
| Wireshark versiones desde la 3.2.0 hasta la 3.2.6, y desde la 3.0.0 hasta la 3.0.13. | |
| **Enlaces para revisar el informe:** | |
| https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00318-01/ | |
| https://www.csirt.gob.cl/media/2020/11/9VSA20-00318-01.pdf | |


| CSIRT comparte actualizaciones de Microsoft en su martes de parche | |
|---|---|
| Alerta de seguridad cibernética | 9VSA20-00319-01 |
| Clase de alerta | Vulnerabilidad |
| Tipo de incidente | Sistema y/o Software Abierto |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 10 de Noviembre de 2020 |
| Última revisión | 10 de Noviembre de 2020 |
| **CVE** | |
| CVE-2020-16970 - CVE-2020-17000 - CVE-2020-17069<br>CVE-2020-16979 - CVE-2020-17004 - CVE-2020-17071<br>CVE-2020-16981 - CVE-2020-17013 - CVE-2020-17078<br>CVE-2020-16982 - CVE-2020-17017 - CVE-2020-17079<br>CVE-2020-16983 - CVE-2020-17019 - CVE-2020-17081<br>CVE-2020-16984 - CVE-2020-17020 - CVE-2020-17082<br>CVE-2020-16985 - CVE-2020-17029 - CVE-2020-17086<br>CVE-2020-16986 - CVE-2020-17030 - CVE-2020-17101<br>CVE-2020-16987 - CVE-2020-17036 - CVE-2020-17102<br>CVE-2020-16988 - CVE-2020-17045 - CVE-2020-17105<br>CVE-2020-16989 - CVE-2020-17049 - CVE-2020-17106<br>CVE-2020-16990 - CVE-2020-17056 - CVE-2020-17107<br>CVE-2020-16991 - CVE-2020-17062 - CVE-2020-17108<br>CVE-2020-16992 - CVE-2020-17063 - CVE-2020-17109<br>CVE-2020-16993 - CVE-2020-17064 - CVE-2020-17110<br>CVE-2020-16994 - CVE-2020-17065 - CVE-2020-17113<br>CVE-2020-16997 - CVE-2020-17066 - CVE-2020-16999<br>CVE-2020-17067<br>Vulnerabilidades adicionales informadas<br>CVE-2020-17042 - CVE-2020-17060 - CVE-2020-17028<br>CVE-2020-17051 - CVE-2020-17061 - CVE-2020-17076<br>CVE-2020-17052 - CVE-2020-17068 - CVE-2020-17087<br>CVE-2020-17048 - CVE-2020-17073 - CVE-2020-17090<br>CVE-2020-17058 - CVE-2020-17074 - CVE-2020-17100<br>CVE-2020-17053 - CVE-2020-17075 - CVE-2020-17104<br>CVE-2020-17022 - CVE-2020-17037 - CVE-2020-17070<br>CVE-2020-17023 - CVE-2020-17044 - CVE-2020-17088<br>CVE-2020-17001 - CVE-2020-17041 - CVE-2020-17077<br>CVE-2020-17007 - CVE-2020-1325 - CVE-2020-17016<br>CVE-2020-17011 - CVE-2020-1599 - CVE-2020-17025<br>CVE-2020-17014 - CVE-2020-16998 - CVE-2020-17040<br>CVE-2020-17018 - CVE-2020-17005 - CVE-2020-17021<br>CVE-2020-17024 - CVE-2020-17006 - CVE-2020-17055<br>CVE-2020-17026 - CVE-2020-17010 - CVE-2020-17085<br>CVE-2020-17031 - CVE-2020-17012 - CVE-2020-17083<br>CVE-2020-17032 - CVE-2020-17027 - CVE-2020-17084<br>CVE-2020-17033 - CVE-2020-17034 - CVE-2020-17091<br>CVE-2020-17035 - CVE-2020-17038 - CVE-2020-17046<br>CVE-2020-17043 - CVE-2020-17047 - CVE-2020-17015<br>CVE-2020-17054 - CVE-2020-17057 | |
| **Fabricante** | |
| Microsoft | |

| Productos afectados |
| --- |
| AV1 Video Extension |
| Azure DevOps Server 2019 Update 1.1 |
| Azure Sphere |
| ChakraCore |
| HEIF Image Extension |
| HEVC Video Extensions |
| Internet Explorer 11 |
| Microsoft 365 Apps for Enterprise (para sistemas 32-bit y 64-bit) |
| Microsoft Dynamics 365 (on-premises) versiones 8.2 y 9.0 |
| Microsoft Dynamics CRM 2015 (on-premises) version 7.0 |
| Microsoft Edge (EdgeHTML-based) |
| Microsoft Excel |
| 2010 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 |
| 2013 Cumulative Update 23 |
| 2016 Cumulative Update 17 |
| 2016 Cumulative Update 18 |
| 2019 Cumulative Update 6 |
| 2019 Cumulative Update 7 |
| 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) |
| 2019 (32-bit y 64-bit editions) |
| 2019 for Mac |
| Online Server |
| Web Apps 2013 Service Pack 1 |
| 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 Teams |
| Microsoft Visual Studio |
| 2017 version 15.9 (includes 15.0 – 15.8) |
| 2019 version 16.0 |
| 2019 version 16.4 (includes 16.0 – 16.3) |
| 2019 version 16.7 (includes 16.0 – 16.6) |
| 2019 version 16.8 |
| 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) |

| |
|---|
| Raw Image Extension<br>Visual Studio Code<br>WebP Image Extension<br>Windows 10 (32-bit y 64-bit)<br>Version 1607, 1709, 1803, 1809, 1903, 1909, 2004, 20H2, para 32 bit, 64 bit y ARM64-based<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 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>x64-based Systems Service Pack 2<br>x64-based Systems Service Pack 2 (Server Core installation)<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 1903 (Server Core installation)<br>version 1909 (Server Core installation)<br>version 2004 (Server Core installation)<br>version 20H2 (Server Core installation) |
| **Enlaces para revisar el informe:** |
| https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00319-01/ |
| https://www.csirt.gob.cl/media/2020/11/9VSA20-00319-01.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 de archivos maliciosos

| |
|---|
| db86e581ed3826fca0c60d9d4ca94108958b39f40b0c0189204988fc9af7f20f |
| 8becdebd3e150c737027e85d7c7764945c3ec196e6b61764eb397a59066a7205 |
| f9c4453d4982a2a34d01e0359894920b0fc51c510e2384c42e21c07ac717656d |
| 42606b1c7c2d7a81362a29f1df26479677baa6daaf0673bb6b8a4b5a36a7dfb4 |
| accaa1abb731482346823f3043cd56bbf7d0067588d2a1f98f2fce96332ab465 |
| 4dda6d1c30ed88737c6b9916e8a2f10c9360fac9495160146aa6e8edd9e4874b |
| 4f11d9da852fcc26a95f8322f011a018c098d852ccec7979a4487c1e6e29f14a |
| a68cb10192709fb2145aa482f4d5d1881865790aa9deb72578f35c9e2da0b4b6 |
| ce970dde48eeff1c69f617e8df801b4bd3f14a5a457b7fd1561a2580313096db |
| e658761468abce5a386b35b1b606ef09035c1d8380c81d6aaa9a43e2e3ffda8 |

## Direcciones Ip de servidor SMTP donde es enviado el correo malicioso

| |
|---|
| 62.12.114.101 |
| 185.136.161.132 |
| 103.153.78.33 |
| 107.179.8.233 |
| 46.26.67.139 |

## Correos electrónicos de donde son enviados los archivos adjunto con malware

| |
|---|
| Gdk7b1EuiIwq5IzwsRwUHsvai@outbound5.angani.co |
| exinsts@gmail.com |
| lutfullah.ansary@aplombtechbd.com |
| cus-exp3@cargoworldconsol.com |
| golasage265@gmail.com |
| carlemau296@gmail.com |
| 8QuE8nWIGXDqSrUHuMwJ6dM@mail.asiatradehub.biz |

# IoC - Ataques de Fuerza Bruta

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado una serie de intentos de acceso a servidores de correos del sector público y privado. Estos ataques de fuerza bruta intentan vulnerar la autenticación del protocolo para transferencia simple de correos (SMTP) para suplantar a los remitentes originales para depositar correos con contenido o enlaces maliciosos en las bandejas de entrada de sus potenciales víctimas.

| IP |
|---|
| 45144177124 |
| 210.92.18.168 |
| 77.40.3.83 |
| 141.98.80.78 |
| 1,77221E+11 |
| 103.89.88.169 |
| 197.159.68.3 |
| 77.40.2.225 |

# Actualidad

## Primer Simposio Ciberseguridad para Funcionarios Públicos

Con el objetivo de contribuir a mantener equipos preparados, informados y actualizados sobre las tendencias en ciberseguridad y amenazas cibernéticas, la Subsecretaría del Interior a través del CSIRT del Gobierno de Chile realizó el Primer Simposio de Ciberseguridad para Funcionarios Públicos.
La actividad, que se llevó a cabo el 12 de noviembre, y contó con la participación de importantes y reconocidos expositores expertos en materia de ciberseguridad de reconocidas empresas nacionales e internacionales que han firmado un convenio de colaboración de ciberseguridad con la Subsecretaría del Interior. Estas organizaciones fueron: Cisco, Deloitte, Fortintet, (ISC)2, Microsoft, 8.8 Computer Security Conference, Alianza Chilena de Ciberseguridad, Banco Interamericano de Desarrollo (BID), IBM y ACTI.


**Es posible ver el Simposio en el en siguiente enlace:**
https://www.youtube.com/watch?v=D2QqodUkWPI&feature=youtu.be

# 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 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.

- Andrés Basoalto
- Felipe Sologuren
- Javier Candia

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2020.11.13 13:10:48 -03'00'