Ministerio del Interior y Seguridad Pública

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

25-06-2021 | Año 3 | N°103

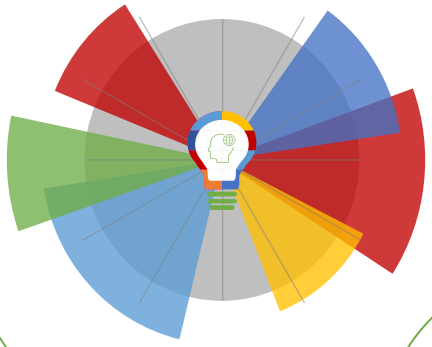
# Boletín de Seguridad Cibernética

Semana del 18 al 24 de junio de 2021

# La semana en cifras

**Hash**
69
**SHA**
Asociadas a múltiples campañas de phishing con archivos que contienen malware

**Se advirtieron**
16
**URL**
Asociadas a sitios fraudulentos y campañas de phishing



**Parches**
5
**para vulnerabilidades**
Las mitigaciones son útiles en productos de Dell y SonicWall.

**IP**
76
**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 ante campaña de malware que suplanta a la Tesorería General de la República | |
|---|---|
| Alerta de seguridad cibernética | 2CMV21-00195-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Malware |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 22 de junio de 2021 |
| Última revisión | 22 de junio de 2021 |
| **Indicadores de compromiso** | |
| SHA256 | |
| D951401CC332CCBC7BE8B50512D13061162FD99E80E11947942273DBDBB4A437<br>77E19EEB9AC37EFB541EF647F401A372F5ED2098690156AE6A42AE65B906DEA6<br>B3B6EE98ACA14CF5BC9F3BC7897BC23934BF85FC4BC25B7506FE4CD9A767047A | |
| **Enlaces para revisar el informe:** | |
| https://www.csirt.gob.cl/alertas/2CMV21-00193-01/ | |
| https://csirt.gob.cl/media/2021/06/2CMV21-00193-01.pdf | |

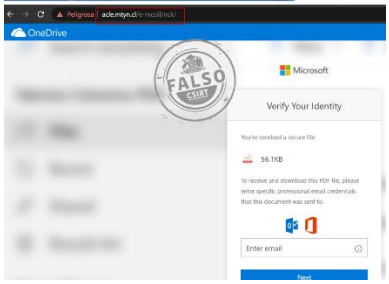

| CSIRT alerta de campaña de malware que suplanta a una empresa | |
|---|---|
| Alerta de seguridad cibernética | 2CMV21-00196-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Malware |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 22 de junio de 2021 |
| Última revisión | 22 de junio de 2021 |
| **Indicadores de compromiso** | |
| SHA256 | |
| 92DC768A4FA5EFD45D9DD6584BF7826EAC025A248E3FDBA637CB4C0848AACD54<br>C69F392D73FFA5B09D2EA03CEFD8E5E7D9A490EF819468DB9409BD9988E26C54 | |
| **Enlaces para revisar el informe:** | |
| https://www.csirt.gob.cl/alertas/2CMV21-00193-01/ | |
| https://csirt.gob.cl/media/2021/06/2CMV21-00193-01.pdf | |

# Sitios fraudulentos

Imagen del sitio

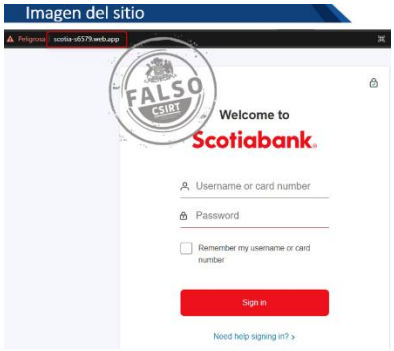

| CSIRT alerta ante página fraudulenta que suplanta a Wells Fargo | |
|---|---|
| Alerta de seguridad cibernética | 8FFR21-00975-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Falsificación de Registros o Identidad |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 22 de junio de 2021 |
| Última revisión | 22 de junio de 2021 |
| **Indicadores de compromiso** | |
| URL sitio falso | |
| https://maximoarte[.]cl/Wells/login.php | |
| IP | |
| [177.221.140.71] | |
| **Enlaces para revisar el informe:** | |
| https://www.csirt.gob.cl/alertas/8ffr21-00975-01/ | |
| https://www.csirt.gob.cl/media/2021/06/8FFR21-00975-01.pdf | |

Imagen del sitio




| CSIRT alerta ante sitio fraudulento que suplanta a OneDrive de Microsoft | |
|---|---|
| Alerta de seguridad cibernética | 8FFR21-00976-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Falsificación de Registros o Identidad |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 22 de junio de 2021 |
| Última revisión | 22 de junio de 2021 |
| **Indicadores de compromiso** | |
| URL sitio falso | |
| https://acle.mtyn[.]cl/e-mcoil/nck/ | |
| IP | |
| [190.96.75.158] | |
| **Enlaces para revisar el informe:** | |
| https://www.csirt.gob.cl/alertas/8ffr21-00976-01/ | |
| https://www.csirt.gob.cl/media/2021/06/8FFR21-00976-01.pdf | |


| CSIRT alerta ante sitio fraudulento que suplanta a Facebook | |
|---|---|
| Alerta de seguridad cibernética | 8FFR21-00977-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Falsificación de Registros o Identidad |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 22 de junio de 2021 |
| Última revisión | 22 de junio de 2021 |
| **Indicadores de compromiso** | |
| URL sitio falso | |
| https://realestate-agent-804708247.mecanizadomds[.]cl/ | |
| IP | |
| [186.64.119.95] | |
| **Enlaces para revisar el informe:** | |
| https://www.csirt.gob.cl/alertas/8ffr21-00977-01/ | |
| https://www.csirt.gob.cl/media/2021/06/8FFR21-00977-01.pdf | |




| CSIRT advierte de página fraudulenta que suplanta al banco Scotiabank | |
|---|---|
| Alerta de seguridad cibernética | 8FFR21-00978-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Falsificación de Registros o Identidad |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 22 de junio de 2021 |
| Última revisión | 22 de junio de 2021 |
| **Indicadores de compromiso** | |
| URL sitio falso | |
| https://scotia-s6579.web[.]app/ | |
| IP | |
| [151.101.65.195] | |
| **Enlaces para revisar el informe:** | |
| https://www.csirt.gob.cl/alertas/8ffr21-00978-01/ | |
| https://www.csirt.gob.cl/media/2021/06/8FFR21-00978-01.pdf | |

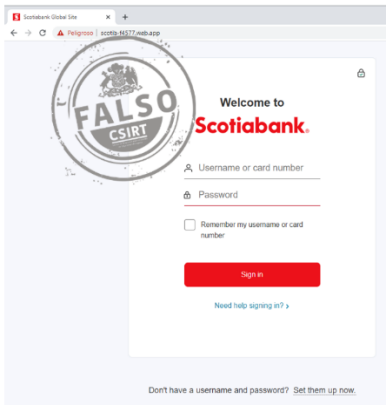
Imagen del sitio


| CSIRT alerta ante página fraudulenta que suplanta a Wells Fargo | |
|---|---|
| Alerta de seguridad cibernética | 8FFR21-00979-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Falsificación de Registros o Identidad |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 23 de junio de 2021 |
| Última revisión | 23 de junio de 2021 |
| **Indicadores de compromiso** | |
| URL sitio falso | |
| https://maximoarte[.]cl/Wells/login.php | |
| IP | |
| [177.221.140.71] | |
| **Enlaces para revisar el informe:** | |
| https://www.csirt.gob.cl/alertas/8ffr21-00979-01/ | |
| https://www.csirt.gob.cl/media/2021/06/8FFR21-00979-01.pdf | |

Imagen del sitio


| CSIRT alerta ante página fraudulenta que suplanta a Office 365 | |
|---|---|
| Alerta de seguridad cibernética | 8FFR21-00980-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Falsificación de Registros o Identidad |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 23 de junio de 2021 |
| Última revisión | 23 de junio de 2021 |
| **Indicadores de compromiso** | |
| URL sitio falso | |
| https://danripley[.]com/viewer/main.html | |
| IP | |
| [209.59.140.34] | |
| **Enlaces para revisar el informe:** | |
| https://www.csirt.gob.cl/alertas/8ffr21-00980-01/ | |
| https://www.csirt.gob.cl/media/2021/06/8FFR21-00980-01.pdf | |

Imagen del sitio




| CSIRT alerta ante sitio fraudulento que suplanta al Scotiabank | |
|---|---|
| Alerta de seguridad cibernética | 8FFR21-00981-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Falsificación de Registros o Identidad |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 23 de junio de 2021 |
| Última revisión | 23 de junio de 2021 |
| **Indicadores de compromiso** | |
| URL sitio falso | |
| https://scotia-f4577[.]web.app/ | |
| IP | |
| [151.101.65.195] | |
| **Enlaces para revisar el informe:** | |
| https://www.csirt.gob.cl/alertas/8ffr21-00981-01/ | |
| https://www.csirt.gob.cl/media/2021/06/8FFR21-00981-01.pdf | |

Imagen del sitio


| CSIRT alerta de una página fraudulenta que suplanta a Office 365 | |
|---|---|
| Alerta de seguridad cibernética | 8FFR21-00982-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Falsificación de Registros o Identidad |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 24 de junio de 2021 |
| Última revisión | 24 de junio de 2021 |
| **Indicadores de compromiso** | |
| URL sitio falso | |
| https://ppi.mwavpn[.]com/ | |
| IP | |
| [52.165.230.236] | |
| **Enlaces para revisar el informe:** | |
| https://www.csirt.gob.cl/alertas/8ffr21-00982-01/ | |
| https://www.csirt.gob.cl/media/2021/06/8FFR21-00982-01.pdf | |

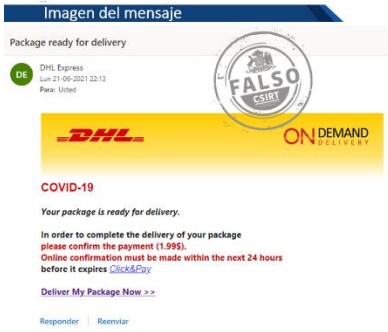
# Phishing

Imagen del mensaje


| CSIRT alerta ante campaña de smishing que suplanta al Banco Santander | |
|---|---|
| Alerta de seguridad cibernética | 8FPH21-00411-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Phishing |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 21 de junio de 2021 |
| Última revisión | 21 de junio de 2021 |
| **Indicadores de compromiso** | |
| URL sitio falso | |
| https://chileseguro[.]app/1624287600/personas/index.asp | |
| IP | |
| [162.213.255.53] | |
| **Enlaces para revisar el informe:** | |
| https://www.csirt.gob.cl/alertas/8fph21-00411-01/ | |
| https://www.csirt.gob.cl/media/2021/06/8FPH21-00411-01.pdf | |

Imagen del mensaje


| CSIRT alerta ante sitio fraudulento que suplanta a Visa y MasterCard | |
|---|---|
| Alerta de seguridad cibernética | 8FPH21-00412-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Phishing |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 22 de junio de 2021 |
| Última revisión | 22 de junio de 2021 |
| **Indicadores de compromiso** | |
| URL sitio falso | |
| https://www.aplusgrader[.]com/.well-known/pageerros/ | |
| IP | |
| [66.235.200.112] | |
| **Enlaces para revisar el informe:** | |
| https://www.csirt.gob.cl/alertas/8fph21-00412-01/ | |
| https://www.csirt.gob.cl/media/2021/06/8FPH21-00412-01.pdf | |




| CSIRT alerta ante campaña de phishing que suplanta a DHL | |
|---|---|
| Alerta de seguridad cibernética | 8FPH21-00413-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Phishing |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 15 de junio de 2021 |
| Última revisión | 15 de junio de 2021 |
| **Indicadores de compromiso** | |
| URL sitio falso | |
| https://website.spicykraft[.]com/DHL/DHL-Express/Shipment/Tracking/ | |
| IP | |
| [104.21.16.144] | |
| **Enlaces para revisar el informe:** | |
| https://www.csirt.gob.cl/alertas/8fph21-00413-01/ | |
| https://www.csirt.gob.cl/media/2021/06/8FPH21-00413-01.pdf | |


| CSIRT alerta por sitio fraudulento que suplanta al Banco Ripley | |
|---|---|
| Alerta de seguridad cibernética | 8FPH21-00414-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Phishing |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 23 de junio de 2021 |
| Última revisión | 23 de junio de 2021 |
| **Indicadores de compromiso** | |
| URL sitio redirección | |
| https://bit[.]ly/3gRWrcB?l=www.bancoripley.cl | |
| https://kukul[.]mx/wp-content/languages/plugins/enviar03.php?l=728736750 | |
| https://bit[.]ly/3gKMSxi?l=www.bancoripley.cl'» | |
| http://185.8.129[.]126/activacion/cuenta-izrp/ | |
| URL sitio falso | |
| http://wwwbancoripley-cl.birdie-golfshop[.]nl/login | |
| IP | |
| [92.48.232.159] | |
| **Enlaces para revisar el informe:** | |
| https://www.csirt.gob.cl/alertas/8fph21-00414-01/ | |
| https://www.csirt.gob.cl/media/2021/06/8FPH21-00414-01.pdf | |

# Vulnerabilidades


| CSIRT alerta por vulnerabilidad grave en SonicWall | |
|---|---|
| Alerta de seguridad cibernética | 9VSA21-00458-01 |
| Clase de alerta | Vulnerabilidad |
| Tipo de incidente | Sistema y/o Software Abierto |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 23 de junio de 2021 |
| Última revisión | 23 de junio de 2021 |
| **CVE** | |
| CVE-2020-5135 | |
| **Fabricante** | |
| SonicWall | |
| **Productos afectados** | |
| SonicOS 6.5.4.6-79n y anteriores | |
| SonicOS 6.5.1.11-4n y anteriores | |
| SonicOS 6.0.5.3-93o y anteriores | |
| SonicOSv 6.5.4.4-44v-21-794 y anteriores | |
| **Enlaces para revisar el informe:** | |
| https://www.csirt.gob.cl/vulnerabilidades/9VSA21-00458-01 | |
| https://www.csirt.gob.cl/media/2021/06/9VSA21-00458.01.pdf | |


| CSIRT alerta ante vulnerabilidades graves en productos Dell | | | |
|---|---|---|---|
| Alerta de seguridad cibernética | 9VSA21-00459-01 | | |
| Clase de alerta | Vulnerabilidad | | |
| Tipo de incidente | Sistema y/o Software Abierto | | |
| Nivel de riesgo | Alto | | |
| TLP | Blanco | | |
| Fecha de lanzamiento original | 24 de junio de 2021 | | |
| Última revisión | 24 de junio de 2021 | | |
| **CVE** | | | |
| CVE-2021-21571 | CVE-2021-21572 | CVE-2021-21573 | CVE-2021-21574 |
| **Fabricante** | | | |
| Dell | | | |
| **Productos afectados** | | | |
| Alienware m15 R6 | AIOInspiron 7706 | Precision 3440 | |
| ChengMing 3990 | 2n1Latitude 3120 | Precision 3450 | |
| ChengMing 3991 | Latitude 3320 | Precision 3550 | |
| Dell G15 5510 | Latitude 3410 | Precision 3551 | |
| Dell G15 5511 | Latitude 3420 | Precision 3560 | |
| Dell G3 3500 | Latitude 3510 | Precision 3561 | |
| Dell G5 5500 | Latitude 3520 | Precision 3640 | |
| Dell G7 7500 | Latitude 5310 | Precision 3650 MT | |
| Dell G7 7700 | Latitude 5310 2 in 1 | Precision 5550 | |
| Inspiron 14 5418 | Latitude 5320 | Precision 5560 | |
| Inspiron 15 5518 | Latitude 5320 2-in-1 | Precision 5760 | |
| Inspiron 15 7510 | Latitude 5410 | Precision 7550 | |
| Inspiron 3501 | Latitude 5411 | Precision 7560 | |

| | | |
|---|---|---|
| Inspiron 3880 | Latitude 5420 | Precision 7750 |
| Inspiron 3881 | Latitude 5510 | Precision 7760 |
| Inspiron 3891 | Latitude 5511 | Vostro 14 5410 |
| Inspiron 5300 | Latitude 5520 | Vostro 15 5510 |
| Inspiron 5301 | Latitude 5521 | Vostro 15 7510 |
| Inspiron 5310 | Latitude 7210 2-in-1 | Vostro 3400 |
| Inspiron 5400 2n1 | Latitude 7310 | Vostro 3500 |
| Inspiron 5400 AIO | Latitude 7320 | Vostro 3501 |
| Inspiron 5401 | Latitude 7320 Detachable | Vostro 3681 |
| Inspiron 5401 AIO | Latitude 7410 | Vostro 3690 |
| Inspiron 5402 | Latitude 7420 | Vostro 3881 |
| Inspiron 5406 2n1 | Latitude 7520 | Vostro 3888 |
| Inspiron 5408 | Latitude 9410 | Vostro 3890 |
| Inspiron 5409 | Latitude 9420 | Vostro 5300 |
| Inspiron 5410 2-in-1 | Latitude 9510 | Vostro 5301 |
| Inspiron 5501 | Latitude 9520 | Vostro 5310 |
| Inspiron 5502 | Latitude 5421 | Vostro 5401 |
| Inspiron 5508 | OptiPlex 3080 | Vostro 5402 |
| Inspiron 5509 | OptiPlex 3090 UFF | Vostro 5501 |
| Inspiron 7300 | OptiPlex 3280 All-in-One | Vostro 5502 |
| Inspiron 7300 2n1 | OptiPlex 5080 | Vostro 5880 |
| Inspiron 7306 2n1 | OptiPlex 5090 Tower | Vostro 5890 |
| Inspiron 7400 | OptiPlex 5490 AIO | Vostro 7500 |
| Inspiron 7500 | OptiPlex 7080 | XPS 13 9305 |
| Inspiron 7500 2n1 – Black | OptiPlex 7090 Tower | XPS 13 2in1 9310 |
| Inspiron 7500 2n1 – Silver | OptiPlex 7090 UFF | XPS 13 9310 |
| Inspiron 7501 | OptiPlex 7480 All-in-One | XPS 15 9500 |
| Inspiron 7506 2n1 | OptiPlex 7490 All-in-One | XPS 15 9510 |
| Inspiron 7610 | OptiPlex 7780 All-i-One | XPS 17 9700 |
| Inspiron 7700 | Precision 17 M5750 | XPS 17 9710 |

**Enlaces para revisar el informe:**

https://www.csirt.gob.cl/vulnerabilidades/9VSA21-00459-01

https://www.csirt.gob.cl/media/2021/06/9VSA21-00459-01.pdf

# IoC Malware

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

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

| Hash de archivos maliciosos | Tipo de malware | Documento web |
|---|---|---|
| fcbb3448283f838450525d95db80b45ae94969df c16d14cb157476b68d22a3d0 | MSIL/GenKryptik.FGTO!tr | 2CMV21-00194-01 |
| f0ccaee0df2bd4ca1adf350dacd3d3c825bce9790 32631fc94f367dfb6b12dde | MSIL/Kryptik.ABOZ!tr | 2CMV21-00194-01 |
| e9112afc22e4ff401301207f5126e09e649b8a27e 5c9d0f954e086a9912768fc | MSIL/Kryptik.ABOX!tr | 2CMV21-00194-01 |
| e54bd099f68d8ca20a70d330fd3c277640e1492f 580197ced70e22e333c8e4af | MSIL/GenKryptik.EYUG!tr | 2CMV21-00194-01 |
| ba2a856a938efc73aca22df09ad27f25ca9f2ee15 7fbfa260ae71799fa86ecbf | RTF/CVE_2017_11882.C! | 2CMV21-00194-01 |
| b71eb2dc0d9b60a63e71b08efb86ad8d7ac87ead 24eff07ab6cf678acfc40745 | HTML/Phish.HHH!tr | 2CMV21-00194-01 |
| a46b0e2949b1e018750f6e45d4eb72db77af1ffe0 82d5a5e3497ee96e2f0bfb1 | MSIL/Kryptik.ABOX!tr | 2CMV21-00194-01 |
| 9d8d459b9dcfe684a6b481c6437527a9286f0b36 a9cdcb5b7b2dc223019bc44c | HTML/Phish.HHH!tr | 2CMV21-00194-01 |
| 889a09da16659cb3c294cc7117304bfdf322e4ca2 dc173d6ce995574fd7501cd | W32/Kryptik.J!tr | 2CMV21-00194-01 |
| 822377d44ed293692824d808c2eb604988764e2 992f176877b47932acf713b1f | W32/Kryptik.J!tr | 2CMV21-00194-01 |
| 7d7df45583e4977ce7d6603e48eded085d0269b 865efb1f864fd8d0f151122ab | MSIL/Kryptik.ABOZ!tr | 2CMV21-00194-01 |
| 68fff3d30ce8b47b353668c6926340428fa22a015 40414876886adc468983c32 | W32/Kryptik.J!tr | 2CMV21-00194-01 |
| 5c8e707f97527fe72d69bc3bcde843a12ed7d249 6c2951cf3fcaef9746027c01 | MSIL/Kryptik.ABPQ!tr | 2CMV21-00194-01 |
| 5754eb30af4f5da98bdc0cb22e01935d1017e8f8 7c65dd85267804783ce6b9e9 | W32/Kryptik.J!tr | 2CMV21-00194-01 |
| 3a0259b1e479db102e0ba166d099d0f88340e26 e16be2867f03e4e84cdbc8e75 | MSIL/Kryptik.ABOZ!tr | 2CMV21-00194-01 |
| 14c8d186fc9223fef35efc0903051fa6f87e896f1f6 361e99a58ebc31bccc825 | MSIL/Kryptik.ABPQ!tr | 2CMV21-00194-01 |
| ff82ab8400ae69ecdfd6b12f00a90a376ffd4e2b38 c8f207b2cebe4c69fbb0c6 | HTML/Phishing.BTV!tr | 2CMV21-00197-01 |

| | | |
|---|---|---|
| f9bc815dc761ae64886b715d53ed9400774d80fc2cedd392ff6c92a200386df5 | HTML/Phishing.BTV!tr | 2CMV21-00197-01 |
| e5be54595d0f9649adc7a917359639e01879d9bdb940c3aec97eb0397277745f | HTML/Phishing.BTV!tr | 2CMV21-00197-01 |
| e2da1a74cf28bf220cdab3669dfae45102deb914ed49376c09c690cd6931f896 | HTML/Phishing.BTV!tr | 2CMV21-00197-01 |
| dd182f749545c253e0464ea70870d13d33dac3704f718e454bda234c620879c4 | HTML/Phishing.BTV!tr | 2CMV21-00197-01 |
| cb6cc6c24c3d2606d042e8cfec2494f5b9ba4dfd9cb50715d6efdf6124e1cd01 | HTML/Phishing.BTV!tr | 2CMV21-00197-01 |
| bf629ec0f816215ea76942f298f22a251b6355a81d525db420f79ecb910514e2 | MSIL/Kryptik.ABOZ!tr | 2CMV21-00197-01 |
| b68546c028d04120cf7ca3ed66cb38299631f25f3b92c499a6a477288d4cb0ee | HTML/Phishing.BTV!tr | 2CMV21-00197-01 |
| a250a37761d0cea3194d1bc27e9101afbd173ee0833f3d189ed07b905ee9407c | HTML/Phishing.BTV!tr | 2CMV21-00197-01 |
| 9ff62acba2b7fed43a83fe2bf9267520f18b74a0daa119cdf591b887220bff75 | HTML/Phishing.BTV!tr | 2CMV21-00197-01 |
| 9bacee9e5a909ff541686d76aaa5d0dd49265db38a64b2a31d45a617d354292f | HTML/Phishing.BTV!tr | 2CMV21-00197-01 |
| 9b33119e625531386211b620784411cc7b4a2346af6e65e2592fbae0c395c7b0 | HTML/Phishing.BTV!tr | 2CMV21-00197-01 |
| 946ce06d94738f5be2434a4c53bfd4ec86902ff7c81bf7c9a4a386176d7a096d | MSIL/Kryptik.ABOZ!tr | 2CMV21-00197-01 |
| 8e79c9a3e42a1b732718757db87936ed7096684101c02024ee55b336ec3e8c69 | HTML/Phishing.BTV!tr | 2CMV21-00197-01 |
| 88d4bbba1a8c58ddb7ea16b1c2e19d0f071a074c8970dccedf99dcca9b1a9157 | HTML/Phishing.BTV!tr | 2CMV21-00197-01 |
| 7dfe609111913d1829761e6e18302062f508f14bd273ed81c21209c8269cb8ad | HTML/Phishing.BTV!tr | 2CMV21-00197-01 |
| 79fd7844545c1c48ae83ec512d61178b6300e9a568ce5342ae0b0f122da56e53 | HTML/Phishing.BTV!tr | 2CMV21-00197-01 |
| 727a37438057780de75601f97953b028c666778e26d38ecfaed979d9ddc77ccd | W32/Malicious_Behavior | 2CMV21-00197-01 |
| 71b03cc0fbeac8169c50a2a13f61836e7ebd3c42fe411ad56841d1b1da9dca74 | HTML/Phishing.BTV!tr | 2CMV21-00197-01 |
| 70d3e54e4e8746b63eebe4be0feb8ab250465835f2e338123fce846ea64d2ff1 | HTML/Phishing.BTV!tr | 2CMV21-00197-01 |
| 66d5ce145d743b2eb70ec5643e32554e00c5a9e6905eed686586bc19032a32ba | HTML/Phishing.BTV!tr | 2CMV21-00197-01 |
| 66b8806a3051cf549c142d40943ce6e2112888184ab4b4bd3140615a82cfff92 | MSIL/Kryptik.ABOZ!tr | 2CMV21-00197-01 |
| 65bab1e74589ae7eaeacecf4e46194cf1e0a32943bd05341a933adab49adf3b3 | HTML/Phishing.BTV!tr | 2CMV21-00197-01 |
| 4bb2d75a230e4172b375eb8789d3ae714dfc957 | HTML/Phishing.BTV!tr | 2CMV21-00197-01 |

| | | |
|---|---|---|
| 44a75921e105252c5c15bba16 | | |
| 482d9ab00ed580fb333496335f7a46d5154b7b517cc2efcbe725ab13a67f1200 | Malicious_Behavior.SB | 2CMV21-00197-01 |
| 3ab01a88c4c00fe682f2aad2b9ff94d4e75ff64b0b8ed1a9acd1d0e3355a67c4 | Malicious_Behavior.SB | 2CMV21-00197-01 |
| 36fa16a1246db6a0ca1afe22caa1f278aa3d4b6f4631741d90e76c653e19c935 | W32/Kryptik.J!tr | 2CMV21-00197-01 |
| 2b6a7eb2447c65f303bd1c541588a2eaa544e4ada33525de709fb078f2c5b77a | HTML/Phishing.BTV!tr | 2CMV21-00197-01 |
| 1e80397baf4fb2fd47dbee46bf226daccc0c34f655fdc0ebbb3f76d9c042e0fe | HTML/Phishing.BTV!tr | 2CMV21-00197-01 |
| 1df471ee084307a29cd0d2a559dcb2ed04baaac5869dad089c1a5eff496f05d8 | HTML/Phishing.BTV!tr | 2CMV21-00197-01 |
| 1d3700687bb2f147671aa33fd732fcee4f7f0758568c071e0a5f99e086f4c5fd | HTML/Phishing.BTV!tr | 2CMV21-00197-01 |
| 199f5195ec9a75db09bb372136f62bb58cde6837538122ff2ba03a2960d8b243 | HTML/Phishing.BTV!tr | 2CMV21-00197-01 |
| 06e9f1049e5d6122d2628d69fc94307b83ae02cc694e8c58b622f04f9e5b8312 | HTML/Phishing.BTV!tr | 2CMV21-00197-01 |
| e039ad43d5a03860c1084d3fce4d2bd65f675dbb4bd12464cf1055290f1d4dac | MSIL/Kryptik.ABQG!tr | 2CMV21-00198-01 |
| 871c057c32e1387433ea174fd5c35088e5815aa31714bdbc5e3b5be214408f4c | MSIL/Kryptik.ABOZ!tr | 2CMV21-00198-01 |
| 871c057c32e1387433ea174fd5c35088e5815aa31714bdbc5e3b5be214408f4c | MSIL/Kryptik.ABOZ!tr | 2CMV21-00198-01 |
| e029321f61c3565028e301eb963c232ce2401f10a82920db99f2eba2501849a5 | MSIL/GenKryptik.FGVA!tr | 2CMV21-00198-01 |
| 3427da1fff4365f332b9849aed6c2eb5623c4ef13d0e6d5cba065d309dfcbfe9 | MSIL/Kryptik.ABQG!tr | 2CMV21-00198-01 |
| e7b2712b6c5132604c589974a7451e8674f6be3a1de080fd02286545a12df9c1 | Riskware/Application | 2CMV21-00198-01 |
| 802fa78ab16729619c99af0c67002ed8043380616f15ea45b8caecc3591c0e59 | MSIL/Kryptik.ABQG!tr | 2CMV21-00198-01 |
| 98bbeb794f6a45293705c46fc0d146cc82849e4dfcdc87f9cc585f3902c2c32a | MSIL/Kryptik.ABQG!tr | 2CMV21-00198-01 |
| bd91083ce01f04c11111c5c33b76552125e1961efbbe15010b1de43349a08843 | VBA/Agent.MDX!tr | 2CMV21-00198-01 |
| a05c75cc33b9e7a07f7fed5462e81d59577a90de4f0460ebea2e11865bd944d5 | MSIL/Kryptik.ABQG!tr | 2CMV21-00198-01 |
| 43e69968519c37a25a74637c92f51f2a63cf248ec87cdd0964503ec2d6641277 | MSIL/GenKryptik.FGSJ!tr | 2CMV21-00198-01 |
| e4a4efa63c7e2291e2ca9b7d7b800b31e9ca7ae9f24f6fa61d8316e6a094cf78 | MSIL/Kryptik.ABQG!tr | 2CMV21-00198-01 |
| f0fd34abd81abede7139b43e4bf7711073003b3e17c2256fbc53cfb809e32579 | W32/Kryptik.J!tr | 2CMV21-00198-01 |

| | | |
|---|---|---|
| 35edc4ac5548dd9038732a66e1e07224438a47a5a0ec29ed19fa4d7a019ade65 | MSIL/Kryptik.ABQG!tr | 2CMV21-00198-01 |
| 3c70e4b1e427c289ae9c16cbdf92d35f1f3098d75809735089a1c302711544e6 | W32/Kryptik.J!tr | 2CMV21-00198-01 |

**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 |
|---|---|---|
| 159.65.37.145 | DIGITALOCEAN-ASN | 2CMV21-00194-01 |
| 212.192.241.37 | Delis LLC | 2CMV21-00194-01 |
| 45.137.22.88 | RootLayer Web Services Ltd. | 2CMV21-00194-01 |
| 185.222.57.226 | RootLayer Web Services Ltd. | 2CMV21-00194-01 |
| 77.247.110.213 | ABC Consultancy | 2CMV21-00194-01 |
| 104.47.32.52 | MICROSOFT-CORP-MSN-AS-BLOCK | 2CMV21-00194-01 |
| 104.47.41.55 | MICROSOFT-CORP-MSN-AS-BLOCK | 2CMV21-00194-01 |
| 195.133.40.101 | Delis LLC | 2CMV21-00194-01 |
| 185.222.57.176 | RootLayer Web Services Ltd. | 2CMV21-00194-01 |
| 136.144.41.208 | Delis LLC | 2CMV21-00194-01 |
| 185.222.57.184 | RootLayer Web Services Ltd. | 2CMV21-00194-01 |
| 195.133.40.64 | Delis LLC | 2CMV21-00194-01 |
| 136.144.41.79 | Delis LLC | 2CMV21-00194-01 |
| 84.38.130.134 | DataClub S.A. | 2CMV21-00194-01 |
| 185.29.10.132 | DataClub S.A. | 2CMV21-00197-01 |
| 40.92.19.105 | MICROSOFT-CORP-MSN-AS-BLOCK | 2CMV21-00197-01 |
| 40.92.19.37 | MICROSOFT-CORP-MSN-AS-BLOCK | 2CMV21-00197-01 |
| 40.92.19.70 | MICROSOFT-CORP-MSN-AS-BLOCK | 2CMV21-00197-01 |
| 40.92.19.72 | MICROSOFT-CORP-MSN-AS-BLOCK | 2CMV21-00197-01 |
| 40.92.19.84 | MICROSOFT-CORP-MSN-AS-BLOCK | 2CMV21-00197-01 |
| 40.92.19.85 | MICROSOFT-CORP-MSN-AS-BLOCK | 2CMV21-00197-01 |
| 40.92.20.53 | MICROSOFT-CORP-MSN-AS-BLOCK | 2CMV21-00197-01 |
| 40.92.20.72 | MICROSOFT-CORP-MSN-AS-BLOCK | 2CMV21-00197-01 |
| 40.92.20.73 | MICROSOFT-CORP-MSN-AS-BLOCK | 2CMV21-00197-01 |
| 40.92.20.82 | MICROSOFT-CORP-MSN-AS-BLOCK | 2CMV21-00197-01 |
| 40.92.20.86 | MICROSOFT-CORP-MSN-AS-BLOCK | 2CMV21-00197-01 |
| 40.92.40.80 | MICROSOFT-CORP-MSN-AS-BLOCK | 2CMV21-00197-01 |

| | | |
|---|---|---|
| 40.92.89.10 | MICROSOFT-CORP-MSN-AS-BLOCK | 2CMV21-00197-01 |
| 40.92.89.12 | MICROSOFT-CORP-MSN-AS-BLOCK | 2CMV21-00197-01 |
| 40.92.89.17 | MICROSOFT-CORP-MSN-AS-BLOCK | 2CMV21-00197-01 |
| 40.92.89.31 | MICROSOFT-CORP-MSN-AS-BLOCK | 2CMV21-00197-01 |
| 40.92.89.34 | MICROSOFT-CORP-MSN-AS-BLOCK | 2CMV21-00197-01 |
| 40.92.89.38 | MICROSOFT-CORP-MSN-AS-BLOCK | 2CMV21-00197-01 |
| 40.92.89.41 | MICROSOFT-CORP-MSN-AS-BLOCK | 2CMV21-00197-01 |
| 40.92.89.43 | MICROSOFT-CORP-MSN-AS-BLOCK | 2CMV21-00197-01 |
| 40.92.89.66 | MICROSOFT-CORP-MSN-AS-BLOCK | 2CMV21-00197-01 |
| 40.92.89.69 | MICROSOFT-CORP-MSN-AS-BLOCK | 2CMV21-00197-01 |
| 40.92.89.75 | MICROSOFT-CORP-MSN-AS-BLOCK | 2CMV21-00197-01 |
| 40.92.89.88 | MICROSOFT-CORP-MSN-AS-BLOCK | 2CMV21-00197-01 |
| 40.92.89.91 | MICROSOFT-CORP-MSN-AS-BLOCK | 2CMV21-00197-01 |
| 40.92.89.93 | MICROSOFT-CORP-MSN-AS-BLOCK | 2CMV21-00197-01 |
| 40.92.89.97 | MICROSOFT-CORP-MSN-AS-BLOCK | 2CMV21-00197-01 |
| 40.92.90.107 | MICROSOFT-CORP-MSN-AS-BLOCK | 2CMV21-00197-01 |
| 40.92.90.15 | MICROSOFT-CORP-MSN-AS-BLOCK | 2CMV21-00197-01 |
| 40.92.90.18 | MICROSOFT-CORP-MSN-AS-BLOCK | 2CMV21-00197-01 |
| 40.92.90.26 | MICROSOFT-CORP-MSN-AS-BLOCK | 2CMV21-00197-01 |
| 40.92.90.36 | MICROSOFT-CORP-MSN-AS-BLOCK | 2CMV21-00197-01 |
| 40.92.90.62 | MICROSOFT-CORP-MSN-AS-BLOCK | 2CMV21-00197-01 |
| 40.92.90.93 | MICROSOFT-CORP-MSN-AS-BLOCK | 2CMV21-00197-01 |
| 40.92.91.48 | MICROSOFT-CORP-MSN-AS-BLOCK | 2CMV21-00197-01 |
| 45.137.22.110 | RootLayer Web Services Ltd. | 2CMV21-00197-01 |
| 64.52.174.67 | CLOUD-SOUTH | 2CMV21-00197-01 |
| 40.92.97.70 | MICROSOFT-CORP-MSN-AS-BLOCK | 2CMV21-00198-01 |
| 209.127.186.54 | SERVER-MANIA | 2CMV21-00198-01 |
| 91.142.222.77 | Infortelecom Hosting S.L. | 2CMV21-00198-01 |
| 162.241.208.223 | UNIFIEDLAYER-AS-1 | 2CMV21-00198-01 |
| 200.29.228.15 | WebHost Chile S.A | 2CMV21-00198-01 |
| 195.133.18.153 | Delis LLC | 2CMV21-00198-01 |
| 92.52.217.3 | Giganet Internet Szolgaltato Kft | 2CMV21-00198-01 |
| 195.133.18.165 | Delis LLC | 2CMV21-00198-01 |
| 185.222.58.148 | RootLayer Web Services Ltd. | 2CMV21-00198-01 |
| 92.52.218.50 | Giganet Internet Szolgaltato Kft | 2CMV21-00198-01 |
| 195.133.18.12 | Delis LLC | 2CMV21-00198-01 |

# Actualidad

## Ciberconsejos | Cómo evitar que tu hijo sea víctima del grooming

En internet existen adultos abusadores que engañar a niños y adolescentes, ganando su amistad para obtener contenido erótico o reunirse con ellos en persona. Conoce más aquí: csirt.gob.cl/recomendaciones/ciberconsejos-como-evitar-que-tu-hijo-sea-victima-del-grooming/.

# 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.

- Elisa Cortez
- Hanz
- José Alfredo Cuevas Ortiz
- Felipe Andrés Hott Delgado
- Alberto Gonzalo Hernández Rodríguez
- Bobby Roe

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2021.06.25 15:22:00 -04'00'