Ministerio del Interior y Seguridad Pública

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

14-05-2021 | Año 3 | N°97

Boletín de Seguridad Cibernética

Semana del 07 al 13 de mayo de 2021

La semana en cifras

Hash

73

SHA

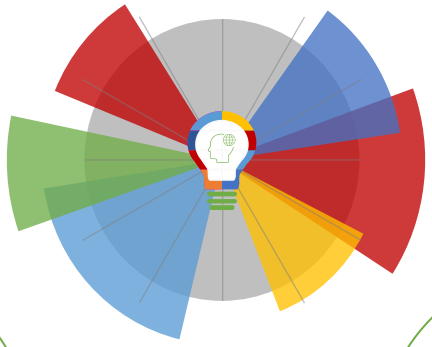
Asociadas a múltiples campañas de phishing con archivos que contienen malware

Se advirtieron

11

URL

Asociadas a sitios fraudulentos y campañas de phishing



Parches

84

para vulnerabilidades

Las mitigaciones son útiles en productos de Red Hat, Microsoft y Google.

IP

55

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.

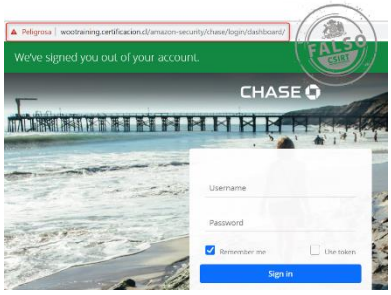
Contenido

Malware

CSIRT alerta por campaña de malware que suplanta a la Tesorería General de la República	
Alerta de seguridad cibernética	2CMV21-00174-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	10 de mayo de 2021
Última revisión	10 de mayo de 2021
Indicadores de compromiso	
SHA256	
9320A80F15B11F981DA5CB831D06408EC6FEE620407202F446BC7A3DAC13794C 9C5E4442E24D03738140EC434D4A5B99367BE5542D71FBD9B5AFEB80008D8643 AB473D07504FBD2E9F071F9ABCD419BAF4671C17D893BCB84F41348CB23D5195 C16C6DEF9C3753EA441E317E16649C0CB6CE9E5544E92B55A97715182D4FC78E 20691095F8E73E8F1910CD88542FF81ADB40B23AF4AF133D7B9CFB2FAA08692E B28479201FC52376BB5C979E562B77695D6DE5A41A14E847B8AF8900BC69ECD2	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2CMV21-00174-01/	

Sitios fraudulentos

Imagen del sitio



CSIRT alerta por sitio fraudulento que suplanta al banco Chase	
Alerta de seguridad cibernética	8FFR21-00946-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	12 de mayo de 2021
Última revisión	12 de mayo de 2021
Indicadores de compromiso	
URL sitio falso	
https://wootraining.certificacion[.]cl/amazon-security/chase/login/dashboard/	
IP	
[200.73.113.241]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-00946-01/	
https://www.csirt.gob.cl/media/2021/05/8FFR21-00946-01.pdf	

Imagen del sitio

CSIRT alerta de sitio fraudulento que suplanta al M&T Bank	
Alerta de seguridad cibernética	8FFR21-00947-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 de mayo de 2021
Última revisión	13 de mayo de 2021
Indicadores de compromiso	
URL sitio falso	
https://agenciarizoma[.]cl/mtb/	
IP	
[167.86.112.84]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-00947-01/	
https://www.csirt.gob.cl/media/2021/05/8FFR21-00947-01.pdf	

Phishing

CSIRT alerta por phishing con email que suplanta al Banco Ripley	
Alerta de seguridad cibernética	8FPH21-00398-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	10 de mayo de 2021
Última revisión	10 de mayo de 2021
Indicadores de compromiso	
URL redirección	
https://bit[.]ly/3tzfuwD?l=www.bancoripley.cl http://evk-keurmeester-arbeidsmiddelen[.]nl/wp-includes/rest-api/enviar03.php?l=67262317 https://bit[.]ly/3xX9j9d?l=www.bancoripley.cl https://virtualnnpa2020[.]com/activacion/cuenta-krnt/	
URL sitio falso	
http://www-bancoripley.cl.oogc[.]ca/login	
IP	
[191.96.151.43]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph21-00398-01/	
https://www.csirt.gob.cl/media/2021/05/8FPH21-00398-01.pdf	

CSIRT alerta por sitio fraudulento que suplanta a Visa y MasterCard	
Alerta de seguridad cibernética	8FPH21-00399-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	10 de mayo de 2021
Última revisión	10 de mayo de 2021
Indicadores de compromiso	
URL redirección	
https://remarkableleading[.]com/LINKKHOOPOODECODEMOMPAMATALHHHTTT.html	
URL sitio falso	
https://assilbeauty[.]com/.well-known/pageerros/50fd202f61fdac536fe7c73d2157b6f6/	
IP	
[162.241.219.14]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph21-00399-01/	
https://www.csirt.gob.cl/media/2021/05/8FPH21-00399-01.pdf	

Imagen del mensaje

CSIRT alerta por phishing con email que suplanta a la Tarjeta Ripley	
Alerta de seguridad cibernética	8FPH21-00400-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	11 de mayo de 2021
Última revisión	11 de mayo de 2021
Indicadores de compromiso	
URL redirección	
http://thekills[.]com/1bc9c5c3e10df97c3b793b5ad9e30402	
URL sitio falso	
https://webripley.cl-jhml[.]com/login	
IP	
[66.29.132.96]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph21-00400-01/	
https://www.csirt.gob.cl/media/2021/05/8FPH21-00400-01.pdf	

Imagen del mensaje

CSIRT alerta por sitio fraudulento que suplanta al Banco de Chile	
Alerta de seguridad cibernética	8FPH21-00401-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	11 de mayo de 2021
Última revisión	11 de mayo de 2021
Indicadores de compromiso	
URL sitio falso	
https://comvoce.britania.com[.]br/0681fb26d19d349ed88368869c39cc64	
IP	
[198.187.29.196]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph21-00401-01/	
https://www.csirt.gob.cl/media/2021/05/8FPH21-00401-01.pdf	

Vulnerabilidades

CSIRT advierte de vulnerabilidades en productos de Red Hat		
Alerta de seguridad cibernética	9VSA21-00442-01	
Clase de alerta	Vulnerabilidad	
Tipo de incidente	Sistema y/o Software Abierto	
Nivel de riesgo	Crítico	
TLP	Blanco	
Fecha de lanzamiento original	12 de mayo de 2021	
Última revisión	12 de mayo de 2021	
CVE		
CVE-2020-28469	CVE-2021-20305	CVE-2021-20305
CVE-2021-23358	CVE-2020-25649	CVE-2021-27363
CVE-2021-28092	CVE-2021-2163	CVE-2021-27364
CVE-2021-29418	CVE-2021-3347	CVE-2021-27365
CVE-2021-28918	CVE-2021-3447	
Fabricante		
Red Hat		
Productos afectados		
Red Hat OpenShift Container Platform 4.6.0 a 4.6.26. Red Hat Advanced Cluster Management for Kubernetes 2.2.0 a 2.2.2		
Enlaces para revisar el informe:		
https://www.csirt.gob.cl/vulnerabilidades/9VSA21-00442-01		
https://www.csirt.gob.cl/media/2021/05/9VSA21-00442-01.pdf		

CSIRT advierte de vulnerabilidades compartidas por Microsoft		
Alerta de seguridad cibernética	9VSA21-00443-01	
Clase de alerta	Vulnerabilidad	
Tipo de incidente	Sistema y/o Software Abierto	
Nivel de riesgo	Alto	
TLP	Blanco	
Fecha de lanzamiento original	11 de mayo de 2021	
Última revisión	11 de mayo de 2021	
CVE		
CVE-2021-26419	CVE-2021-31193	CVE-2021-31173
CVE-2020-24588	CVE-2021-31192	CVE-2021-31172
CVE-2020-24587	CVE-2021-31191	CVE-2021-31171
CVE-2021-31204	CVE-2021-31190	CVE-2021-31170
CVE-2021-26422	CVE-2021-31188	CVE-2021-31169
CVE-2021-26421	CVE-2021-31187	CVE-2021-31168
CVE-2021-31936	CVE-2021-31186	CVE-2021-31167
CVE-2021-31214	CVE-2021-31185	CVE-2021-31166
CVE-2021-31213	CVE-2021-31184	CVE-2021-31165
CVE-2021-31211	CVE-2021-31182	CVE-2021-26418
CVE-2021-31209	CVE-2021-31181	CVE-2021-28479
CVE-2021-31200	CVE-2021-31180	CVE-2021-28478
CVE-2021-31208	CVE-2021-31179	CVE-2021-28476
CVE-2021-31207	CVE-2021-31178	CVE-2021-28474
CVE-2021-31205	CVE-2021-31177	CVE-2021-28461

CVE-2021-28465 CVE-2021-31198 CVE-2021-31195 CVE-2021-31194	CVE-2021-31176 CVE-2021-31175 CVE-2021-31174	CVE-2021-28455 CVE-2020-26144 CVE-2021-27068

Fabricante
Microsoft
Productos afectados
.NET 5.0 .NET Core 3.1 common_utils.py Dynamics 365 for Finance and Operations Internet Explorer 11 Internet Explorer 9 Microsoft 365 Apps for Enterprise for 32-bit Systems Microsoft 365 Apps for Enterprise for 64-bit Systems Microsoft Accessibility Insights for Web Microsoft Excel 2013 RT Service Pack 1 Microsoft Excel 2013 Service Pack 1 (32-bit editions) Microsoft Excel 2013 Service Pack 1 (64-bit editions) Microsoft Excel 2016 (32-bit edition) Microsoft Excel 2016 (64-bit edition) Microsoft Exchange Server 2013 Cumulative Update 23 Microsoft Exchange Server 2016 Cumulative Update 19 Microsoft Exchange Server 2016 Cumulative Update 20 Microsoft Exchange Server 2019 Cumulative Update 8 Microsoft Exchange Server 2019 Cumulative Update 9 Microsoft Lync Server 2013 CU10 Microsoft Office 2013 RT Service Pack 1 Microsoft Office 2013 Service Pack 1 (32-bit editions) Microsoft Office 2013 Service Pack 1 (64-bit editions) Microsoft Office 2016 (32-bit edition) Microsoft Office 2016 (64-bit edition) Microsoft Office 2019 for 32-bit editions Microsoft Office 2019 for 64-bit editions Microsoft Office 2019 for Mac Microsoft Office Online Server Microsoft Office Web Apps Server 2013 Service Pack 1 Microsoft SharePoint Enterprise Server 2016 Microsoft SharePoint Foundation 2013 Service Pack 1 Microsoft SharePoint Server 2019 Microsoft Visual Studio 2019 version 16.4 (includes 16.0 – 16.3) Microsoft Visual Studio 2019 version 16.7 (includes 16.0 – 16.6) Microsoft Visual Studio 2019 version 16.9 (includes 16.0 – 16.8) Microsoft Word 2013 RT Service Pack 1 Microsoft Word 2013 Service Pack 1 (32-bit editions) Microsoft Word 2013 Service Pack 1 (64-bit editions) Microsoft Word 2016 (32-bit edition) Microsoft Word 2016 (64-bit edition) Skype for Business Server 2015 CU11 Skype for Business Server 2019 CU5 Visual Studio 2019 for Mac version 8.9

Visual Studio Code
Visual Studio Code Remote – Containers Extension
Web Media Extensions
Windows 10 for 32-bit Systems
Windows 10 for x64-based Systems
Windows 10 Version 1607 for 32-bit Systems
Windows 10 Version 1607 for x64-based Systems
Windows 10 Version 1803 for 32-bit Systems
Windows 10 Version 1803 for ARM64-based Systems
Windows 10 Version 1803 for x64-based Systems
Windows 10 Version 1809 for 32-bit Systems
Windows 10 Version 1809 for ARM64-based Systems
Windows 10 Version 1809 for x64-based Systems
Windows 10 Version 1909 for 32-bit Systems
Windows 10 Version 1909 for ARM64-based Systems
Windows 10 Version 1909 for x64-based Systems
Windows 10 Version 2004 for 32-bit Systems
Windows 10 Version 2004 for ARM64-based Systems
Windows 10 Version 2004 for x64-based Systems
Windows 10 Version 20H2 for 32-bit Systems
Windows 10 Version 20H2 for ARM64-based Systems
Windows 10 Version 20H2 for x64-based Systems
Windows 7 for 32-bit Systems Service Pack 1
Windows 7 for x64-based Systems Service Pack 1
Windows 8.1 for 32-bit systems
Windows 8.1 for x64-based systems
Windows RT 8.1
Windows Server 2008 for 32-bit Systems Service Pack 2
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core Installation)
Windows Server 2008 for x64-based Systems Service Pack 2
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core Installation)
Windows Server 2008 R2 for x64-based Systems Service Pack 1
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core Installation)
Windows Server 2012
Windows Server 2012 (Server Core installation)
Windows Server 2012 R2
Windows Server 2012 R2 (Server Core installation)
Windows Server 2016
Windows Server 2016 (Server Core installation)
Windows Server 2019
Windows Server 2019 (Server Core installation)
Windows Server, version 1909 (Server Core installation)
Windows Server, version 2004 (Server Core installation)
Windows Server, version 20H2 (Server Core Installation)
Enlaces para revisar el informe:
https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00435-01
https://www.csirt.gob.cl/media/2021/05/9VSA21-00435-01.pdf

CSIRT advierte de vulnerabilidades en productos de Apple		
Alerta de seguridad cibernética	9VSA21-00444-01	
Clase de alerta	Vulnerabilidad	
Tipo de incidente	Sistema y/o Software Abierto	
Nivel de riesgo	Alto	
TLP	Blanco	
Fecha de lanzamiento original	12 de mayo de 2021	
Última revisión	12 de mayo de 2021	
CVE		
CVE-2021-30520	CVE-2021-30515	CVE-2021-30510
CVE-2021-30519	CVE-2021-30514	CVE-2021-30509
CVE-2021-30518	CVE-2021-30513	CVE-2021-30508
CVE-2021-30517	CVE-2021-30512	CVE-2021-30507
CVE-2021-30516	CVE-2021-30511	CVE-2021-30506
Fabricante		
Google		
Productos afectados		
Google Chrome 87.0.4280.66 a 90.0.4430.93		
Enlaces para revisar el informe:		
https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00444-01		
https://www.csirt.gob.cl/media/2021/05/9VSA21-00444-01.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	Documento web
f8a1e977ba90a5621e67a1b04ca4740893ff4279ec4712eb22d8267a0c3a01de	2CMV21-00175-01
f773364cd11c5155ccad0e4d3ed770a0ece02e81a6372f23fc285bdd9f301b0f	2CMV21-00175-01
f00763eaa902104adfc7cb5ff64dfe6fde7ad2069f78f9125de5993f3f1226c6	2CMV21-00175-01
e9d949a4df2e374fee8983e43e0e78cdc49faf0afbed9160b3aea898f0155f2c	2CMV21-00175-01
e9cec5347ad80420939f1fedcdb7d321ee7cbf79ef22f41c860cbc4f668772bb	2CMV21-00175-01
e52cfd603333173f5a5fe560e256dbd05389a09b86ddde41808a748506f3aa44	2CMV21-00175-01
df64df82b18e852a3b662b4b26e46a1077fd298c0b9133ba7a8f084b988a4b0f	2CMV21-00175-01
cfa82fecc8818cf2dd19a0a21c51794fdb62719bffa121ee28bfa79e7b859490	2CMV21-00175-01
cb678fece33a4de8aabc9d527a8188a407dc6432072b9a1cc4f293028dd335ac	2CMV21-00175-01
c031dd1d1ef57bdc41821dc77387ef4f3db03defe3e0979e5993456130d03fb9	2CMV21-00175-01
bbe05176a0d58aefdf00b3d58227f923e20d66c140157d2e804c460db6bf73af	2CMV21-00175-01
bbd1bb83290480d23e3246704ae43deea19e8fd310630a3e4b23639a1530fd5a	2CMV21-00175-01
ba77c9c1a124c51af298551e5d4fb90e5b9ac1b37d835d8cf1e6521bd9ee4f53	2CMV21-00175-01
a2b084545d31feaff2d64383b0d3aad3d380c5b44c65f24ed05aede02e9ad410	2CMV21-00175-01
a2907290b9082b133e5f4d82407976db26620a692834195cbf6a334061c76367	2CMV21-00175-01
a2442bb8a9aeb8af98ccfb07ad9afd62bdbedeb942971a8644d63687dbb65490	2CMV21-00175-01
9abfb60a643a4db9a7013e6560270f355f2f71d09eb294603d22649195d49f95	2CMV21-00175-01
971bd748d074f5233dbea165c1b6db2afad91f05ff898042895d2d2051d28325	2CMV21-00175-01
02fab97fe9b0e2e94abd4917fb5bc88d21445760ee37971b919f47c95a01f195	2CMV21-00176-01
0cbb6c8b7bf0f108b82ac808211852dac62709ceefb84d8e93b2ef912428d24b	2CMV21-00176-01
1ebb93102f8b08f724aad0bd312006450853d65266c0558a88da622d75c67bd8	2CMV21-00176-01
23e012a59ae4794e05bd5de9b353f788d9b9ce7045ca27ff5a93b7b922746db4	2CMV21-00176-01
2775248702bf6bfc3b01f77ace8b5be9f5281eb9e00a6b92323ea4cdca78b2ab	2CMV21-00176-01
33fa7ababe331e58c82f5ca9423f269d598f321c3e8f700373775bc6c993992d	2CMV21-00176-01
389f593eff1b5bc4c552f9765ac8b5070f910428b430a4fc16ca6f8379128a52	2CMV21-00176-01
4b922b87034981af8f69326f64789363ef2b468fc58ddad34c16c5c6bd82e3ca	2CMV21-00176-01
4cedb439d35ae9db6b9f25b013c9d7c0bcee78990305bc0764d245c70b0c86b0	2CMV21-00176-01
4e2543aba8686312bc8212b9c799dc233f91d017b5767e91c5fae744d75d152b	2CMV21-00176-01

5116d89d1fbc3cf87e842b52acd91b70d1cf5a9cd68157fc9ecf9d1b8d3c498c	2CMV21-00176-01
5f4e4fbde7ed003dc34954ee301977f697de1cd2d52beafd898023797ab47255	2CMV21-00176-01
65d09004525ac8e3d844232e6f1f99ec26bcf3a24447ee4a55ef0cf805ca0480	2CMV21-00176-01
65f0e0590469268511ed7b779808f4178386b7d81ad0447d3ae9b5260a42a4d2	2CMV21-00176-01
67cc5fdee7630da23e8b6b63bd6da843cd7ea1e0fe05f47c2dc57bab10716342	2CMV21-00176-01
692d2b764da8c746e7abdcb6d09fc5fa92de2729ddab5fbaa22c42155b9df273	2CMV21-00176-01
6bd884cbbae349fb1933fb97280d2d84a2b71f8adf6c9feb363941c04bb40ef4	2CMV21-00176-01
71daea6f6dedd5094544dec50a02050559328113afe48df41c93a42ce56e855c	2CMV21-00176-01
757e11cf6260b6d84410f18cf27cfb50447e15059fffa296add2469967182d57	2CMV21-00176-01
7e80eb8594da599e745dc646a4fe02aca27c56457aca6a9c35f387c281202c9c	2CMV21-00176-01
84f5938bf6b3849d4055c64663e26912dd368506a5ca784ebccdfe39cf6cde10	2CMV21-00176-01
878a4f96c80d638d087347f2f4d9fd09df01b3bff20ce362c9fff16bca94e5bb	2CMV21-00176-01
95f7f656ee4dee95a46e971797962bc365f9289923a936d2a9b8190bed88b611	2CMV21-00176-01
976d036150ddef649c0fdffa89bfcaa19f5743e98e45d9cdccb76b66632c8ee5	2CMV21-00176-01
9b82331902103e80ae6cdda02fa33bdd00cba59bac68c5d6f1109d1b93020e23	2CMV21-00176-01
a33d4b647cd9a415a96aa0aaa97bbaf2abf2817cf5eef4faf812a3216e9d1a9e	2CMV21-00176-01
a3d4f2e5e5c91a17786c7c3cea524a17d513735550b30b3d4494fc11d6e1135d	2CMV21-00176-01
b38df877b327db04dfa2bea03a94ceec82b1942560acfb6c87256be88f707bb2	2CMV21-00176-01
c3241d3e58071c903d635550d9dd35da14d3602a349c716527e4a9f147b7e4be	2CMV21-00176-01
c3333735a22b46fa116054c15ea6f273bbbcedef13b633d0b7721d91a57ba2b4	2CMV21-00176-01
c53c03a021b14ae039a3115115fdd552892ad3e2e19698492c14121dd582ee07	2CMV21-00176-01
ca91a8dd6f50202cdc5ed444cb1c1f447f2dc108f2c276658f337c93259fb1ce	2CMV21-00176-01
d109452c99cd984de885f08d3be104145f9d4f5396c2001fd6e048c5ffcbfb3d	2CMV21-00176-01
d18e005fa449ab6ac3b7febb25dd6a05e16dc7a87f684ed49d6c093a2c61e6c7	2CMV21-00176-01
d8cbbb4144d9b4350b367fa89b250b4a35933b77c00d36b3e885f2aa17e0aaff	2CMV21-00176-01
d9507b9760fb0ab4ad0a6ca6e92bdbb16cccd5ce1d5e60cf158dc21114092ff4	2CMV21-00176-01
e01ebff50cac856b458473e4e7b47ef942fd93d4327ff8f56bd95a43d954bb3a	2CMV21-00176-01
e55e03e26e7a9c71f639f9aaf6a3c5dfd0138fa4578f9f86d7fce950027d6d2e	2CMV21-00176-01
e79c26ed16f145a7282b54b3137f09e4100495c7d06c0ea73052762d0877dbd3	2CMV21-00176-01
e943753978e4c47b5bca140cbcc1e669b7d900fbe3e55fd37aa1b4925c11fd93	2CMV21-00176-01
eb797eaf04038f3b1330dc4cf7dbfcaca0758a0340082fa223f5399209acb984	2CMV21-00176-01
ed30c09693df6de5d1ceff9395eb0c8662ffbcd5f8fdaf641f9d4df9e77910de	2CMV21-00176-01
f74ad88b84c59f91ebb58052bb7b9a1238a93f86f19f6d9015839d38d26f4364	2CMV21-00176-01
fbc3fb202e26f02612903679f57dd9406546cb79e18d2a0fb31459a276aabe93	2CMV21-00176-01
fd6ade6040d775af6ddf8c835a1f7b32bb17ccaf5ca227af55df9accfc75329d	2CMV21-00176-01

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
146.82.91.211	Adexus S.A.	2CMV21-00175-01
185.222.57.229	RootLayer Web Services Ltd.)	2CMV21-00175-01
143.198.61.188	DIGITALOCEAN-ASN	2CMV21-00175-01
217.146.81.63	Hyonix LLC	2CMV21-00175-01
190.98.225.43	Gtd Internet S.A.	2CMV21-00175-01
103.139.44.91	VIETNAM POSTS AND TELECOMMUNICATIONS GROUP	2CMV21-00175-01
143.110.225.122	DIGITALOCEAN-ASN	2CMV21-00175-01
31.210.20.71	Des Capital B.V.	2CMV21-00175-01
103.151.122.176	VIETNAM POSTS AND TELECOMMUNICATIONS GROUP	2CMV21-00175-01
103.139.44.129	VIETNAM POSTS AND TELECOMMUNICATIONS GROUP	2CMV21-00175-01
31.210.21.118	Des Capital B.V.	2CMV21-00175-01
23.106.122.190	Leaseweb Asia Pacific pte. ltd.	2CMV21-00175-01
103.28.70.140	Hyonix LLC	2CMV21-00175-01
45.144.225.21	Des Capital B.	2CMV21-00175-01
45.12.213.248	Zomro B.V.	2CMV21-00175-01
46.183.221.116	DataClub S.A.	2CMV21-00175-01
45.137.22.149	RootLayer Web Services Ltd.	2CMV21-00176-01
92.42.36.95	EUROTA INTERNET SERVICES LTD	2CMV21-00176-01
185.121.120.179	Serverion BV	2CMV21-00176-01
162.241.205.153	Unified Layer	2CMV21-00176-01
45.137.22.147	RootLayer Web Services Ltd.	2CMV21-00176-01
91.212.89.57	UZINFOCOM State Unitary Enterprise	2CMV21-00176-01
186.65.73.138	Adexus S.A.	2CMV21-00176-01
45.87.60.140	Hyonix	2CMV21-00176-01
103.145.254.33	MAINT-VN-VNNIC	2CMV21-00176-01
77.247.110.104	PEENQ.NL	2CMV21-00176-01
66.36.234.110	HopOne Internet Corporation	2CMV21-00176-01
103.99.1.238	MAINT-VN-VNNIC	2CMV21-00176-01
31.210.21.71	Serverion BV	2CMV21-00176-01
45.170.245.119	ZEROPING S. DE R.L. DE C.V.	2CMV21-00176-01
104.47.33.54	Microsoft Corporation	2CMV21-00176-01
162.241.211.105	Unified Layer	2CMV21-00176-01
181.119.65.95	IFX Networks Argentina S.R.L.	2CMV21-00176-01

104.47.56.48	Microsoft Corporation	2CMV21-00176-01
31.210.20.250	Serverion BV	2CMV21-00176-01
31.210.21.247	Serverion BV	2CMV21-00176-01
185.222.58.100	bd-rootlayer-1-mnt	2CMV21-00176-01
185.29.8.26	DataClub S.A.	2CMV21-00176-01
190.15.202.141	Informática y Telecomunicaciones S.A.	2CMV21-00176-01
103.156.92.46	MAINT-VN-VNNIC	2CMV21-00176-01
45.137.22.52	RootLayer Web Services Ltd.	2CMV21-00176-01
185.121.120.245	Serverion BV	2CMV21-00176-01
153.122.55.69	MAINT-JPNIC	2CMV21-00176-01
185.222.57.174	bd-rootlayer-1-mntB8B2:B28B1:B28	2CMV21-00176-01

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), con el fin de suplantar un remitente original y así depositar correos con contenido o enlaces maliciosos en las bandejas de entrada de sus potenciales víctimas.

IP	Etiqueta de sistema autónomo	Documento web
45.148.10.190	Pptechnology Limited	4IIA21-00037-01
87.246.7.227	Internet Hosting LTD	4IIA21-00037-01
27.255.90.113	EHOSTICT	4IIA21-00037-01
193.29.187.121	THC Projects SRL	4IIA21-00037-01
185.24.233.118	Sternforth Ltd	4IIA21-00037-01

Actualidad

Exitosa primera edición de 8.8 Gobierno reúne una gran audiencia gracias a sus importantes expositores internacionales

El jueves 13 de mayo tuvo lugar la primera conferencia 8.8 dedicada al trabajo de ciberseguridad y ciberinteligencia de los gobiernos e instituciones de carácter nacional. Hecha de forma virtual, contó con invitados de Latinoamérica, Israel, España y Estonia, y logró reunir a **más de mil** espectadores. La conferencia fue abierta por el Ministro del Interior y Seguridad Pública, **Rodrigo Delgado**, tras lo cual comenzó su exposición el director nacional del CSIRT de Gobierno, **Carlos Landeros**, quien detalló de qué se tratan y cómo minimizar el riesgo de sufrir un ataque de cadena de suministro.

Siguieron con charlas el director del **CERT de Estonia, Tõnu Tammer**, con un resumen de las amenazas más peligrosas del último tiempo y algunas herramientas gratuitas para protegernos contra ellas, y el **Centro Criptológico Nacional (CCN) de España**, que presentó todo sobre la OSINT, por ejemplo, formas para detectar sitios de fraude y técnicas para reducir nuestra huella digital.

Luego correspondió el turno de **Mateo Martínez**, director de Krav Maga Hacking, quien comentó desde Uruguay las últimas filtraciones de datos en Latinoamérica y casos de ransomware, y compartió sitios para protegerse del uso de técnicas de scrapping. **Javier Smaldone** siguió con una demostración de los numerosos riesgos del voto electrónico para la integridad de las elecciones, como la falta de comprobación independiente y la pérdida del secreto del voto. “No hay un sistema de votación electrónica que se haya demostrado seguro o confiable”, explicó.

Subsecretario del Interior, Juan Francisco Galli

Ya por la tarde fue el turno del panel de expertas latinoamericanas en ciberseguridad, quienes hablaron diversos temas. **Alison Treppel** (secretaria ejecutiva del Comité Interamericano contra el Terrorismo de la OEA) recalcó las diferencias que enfrentan las mujeres que quieren trabajar en este rubro, mientras **María José Jarquín** (la especialista líder en Modernización del BID) destacó la importancia de aumentar la representación de la mujer en ciberseguridad y con ello facilitar la concientización de las usuarias

Carlos Landeros, director nacional del CSIRT de Gobierno

Un problema es la brecha salarial existente, señaló **Silvia Batista** (directora del CERT Panamá), además de la importancia de acercar a la mujer a los talentos digitales y **Gabriela Ratti** (directora general de Ciberseguridad y Protección de la Información de Paraguay) mencionó también el tema cultural, ya que las redes e instancias de reuniones puramente masculinas excluyen a las mujeres en muchos rubros, siendo la informática uno de los más afectados.

Tõnu Tammer, director del CERT de Estonia.

Treppel resaltó el déficit de 900 mil puestos de ciberseguridad en las Américas, y que debemos apuntar a que la mitad de ellos sea cubierta por mujeres, para lo que se les debe capacitar adecuadamente, y motivarlas a ser parte de esta profesión. Finalmente, el representante del **CERT de Israel** analizó la campaña MuddyWater, la forma en que este grupo logró explotar vulnerabilidades conocidas y phishing para ganar control de equipos clave, las maneras en que logró hacer de su ataque uno persistente, cómo fue posible detectar las web shells en los sistemas vulnerados, entre otros detalles.

El cierre del evento estuvo a cargo del Subsecretario del Interior, **Juan Francisco Galli**.

Ciberconsejos para evitar los peligros del smishing

El smishing es una estafa digital consistente en el envío de SMS o WhatsApp de mensajes que parecen legítimos, pero son falsos y buscan hacernos descargar un malware, o visitar un sitio fraudulento para obtener información personal o robar nuestras cuentas:
https://www.csirt.gob.cl/recomendaciones/ciberconsejos-para-evitar-los-peligros-del-smishing/

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 de este.

- Santiago Lois Martínez Naranjo
- Jholiza Quecaño
- Nehemias Valdebenito Iturra
- Constanza Núñez Barraza
- David Cordovez
- Milagros de Miau

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2021.05.20 11:55:31 -04'00'