Ministerio del Interior y Seguridad Pública

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

20-05-2021 | Año 3 | N°98

Boletín de Seguridad Cibernética

Semana del 14 al 19 de mayo de 2021

La semana en cifras

Hash

118

SHA

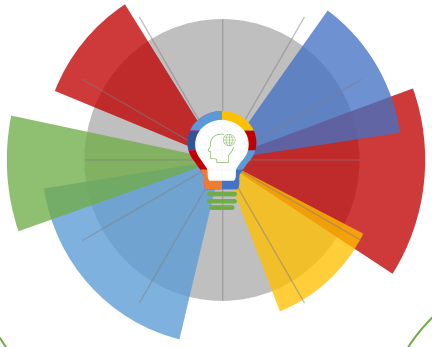
Asociadas a múltiples campañas de phishing con archivos que contienen malware

Se advirtieron

6

URL

Asociadas a sitios fraudulentos y campañas de phishing



Parches

6

para vulnerabilidades

Las mitigaciones son útiles en productos de Red Hat.

IP

84

Informadas

Listado de IP advertidas en múltiples campañas de phishing y de malware.

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

Contenido

Sitios fraudulentos

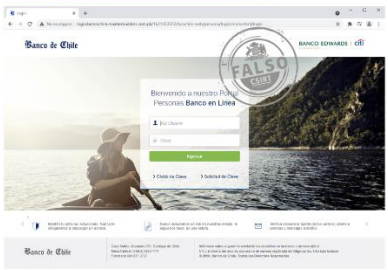
CSIRT alerta por sitio fraudulento que suplanta a Dropbox	
Alerta de seguridad cibernética	8FFR21-00948-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de mayo de 2021
Última revisión	14 de mayo de 2021
Indicadores de compromiso	
URL sitio falso	
https://carlosmena[.]cl/wp-admin/drp/dropbox2mpage/db/view/download.html#	
IP	
[131.72.236.38]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-00948-01/	
https://www.csirt.gob.cl/media/2021/05/8FFR21-00948-01.pdf	

CSIRT alerta por sitio fraudulento que suplanta al Banco Ripley	
Alerta de seguridad cibernética	8FFR21-00949-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de mayo de 2021
Última revisión	14 de mayo de 2021
Indicadores de compromiso	
URL sitio falso	
https://srv.proactivesolucioneslegales[.]cl/login	
IP	
[200.63.99.33]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-00949-01/	
https://www.csirt.gob.cl/media/2021/05/8FFR21-00949-01.pdf	

CSIRT alerta por sitio fraudulento que suplanta a Facebook	
Alerta de seguridad cibernética	8FFR21-00950-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de mayo de 2021
Última revisión	14 de mayo de 2021
Indicadores de compromiso	
URL sitio falso	
https://realestate-agent-290751038.steelwork[.]cl/	
IP	
[186.64.119.35]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-00950-01/	
https://www.csirt.gob.cl/media/2021/05/8FFR21-00950-01.pdf	

CSIRT alerta por sitio fraudulento que suplanta al Banco Ripley	
Alerta de seguridad cibernética	8FFR21-00951-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de mayo de 2021
Última revisión	14 de mayo de 2021
Indicadores de compromiso	
URL sitio falso	
https://srv.proactivesolucioneslegales[.]cl/login	
IP	
[200.63.99.33]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-00951-01/	
https://www.csirt.gob.cl/media/2021/05/8FFR21-00951-01.pdf	

Imagen del sitio



CSIRT alerta por página fraudulenta que suplanta al Banco de Chile	
Alerta de seguridad cibernética	8FFR21-00952-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	18 de mayo de 2021
Última revisión	18 de mayo de 2021
Indicadores de compromiso	
URL sitio falso	
http://login.bancochile.maaherbuilders.com[.]pk/1621353328/bcochile-web/persona/login/index.html/login	
IP	
[51.195.206.62]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-00952-01/	
https://www.csirt.gob.cl/media/2021/05/8FFR21-00952-01.pdf	

Imagen del sitio

CSIRT alerta por página fraudulenta que suplanta a TVN	
Alerta de seguridad cibernética	8FFR21-00953-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	19 de mayo de 2021
Última revisión	19 de mayo de 2021
Indicadores de compromiso	
URL sitio falso	
https://orionsmarketing[.]com/900112/	
IP	
[172.67.74.96]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-00953-01/	
https://www.csirt.gob.cl/media/2021/05/8FFR21-00953-01.pdf	

Vulnerabilidades

CSIRT alerta de vulnerabilidades en Red Hat OpenShift Container Platform	
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	17 de mayo de 2021
Última revisión	17 de mayo de 2021
CVE	
CVE-2020-15586 CVE-2020-16845 CVE-2020-28362 CVE-2021-2163 CVE-2021-3114 CVE-2021-3121	
Fabricante	
Red Hat	
Productos afectados	
Red Hat OpenShift Container Platform 4.7.0 a 4.7.8	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9VSA21-00445-01	
https://www.csirt.gob.cl/media/2021/05/9VSA21-00445-01.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
0cf6394ec7b68f681552642c14242fbfb5cf2ea52a73e70d7f1e4ac5f6ed036d	2CMV21-00177-01
14d711f2f97db7347ebce7e6f289b7d5174a4a9e6a0bc2f4e5a597ef08f652bb	2CMV21-00177-01
172bc04929c268238274133fd4c6accfda36524861d774030c7f86433ccac854	2CMV21-00177-01
18c3d4686dc7aea4ecec07c7f1930e39095917f512051ea15cb3febedea4c4b3	2CMV21-00177-01
1e068e350ecf76279932c4c8cfc7a26c1cdfb27d71bef300c7bb32f9ee77cd3e	2CMV21-00177-01
1e8e3cfe10c00f1ccd82b54857c5c531f6f262cf24e80a6ce67fb628f41e26be	2CMV21-00177-01
27ea000431417515aa33d53ae175d1decb83d151f950d7b2f22aff9fc1e9fc2e	2CMV21-00177-01
291da38191d5ff579484d4fe33aa922f5ee289b2f2a70c95025e5c055a53b354	2CMV21-00177-01
34b8e2ff84e15256bbd27c1679e04f5e37a706fd364ab48734ee629592fffa43	2CMV21-00177-01
39b9b9d746615f349d1dd9bd9d29897a3261fac310d55558e51061edc9886dfc	2CMV21-00177-01
3f656d77229f0f30156f9f3f25019c1b542f02f0236c61e975685910529cbdb8	2CMV21-00177-01
4687cb6cdc7938fab151f4adaade6d848b2896186aa3aa7c6fda30ce2b070872	2CMV21-00177-01
4f0f0e3eb0b053dd9d9f5324e667c74872d43f2f362ed82e9080854a06d4e583	2CMV21-00177-01
504aa616071d68016724490c96f2ab9f1bdbbbba639d4f9380e07c3a47814af3	2CMV21-00177-01
523c55e8eb17fb49b3007915dd26d98cda307a6cd8ebe007bcfcfcebd71402a3	2CMV21-00177-01
5f176553348ef0003ce6cb08a7c480b504b5303abdd522814c31b8e46f328005	2CMV21-00177-01
651669b20fdf67366006b67266c171a3f784c111d94fd3b091c0b7e2f3a12ee4	2CMV21-00177-01
687322df86dd333a2e53f4359642ed378030880d18c08d7d75cf33bfa83bcdf4	2CMV21-00177-01
6fc656c9d0d087d4404a5a32b663f8861b7c2cf71de7c80d6538e0702fe51d45	2CMV21-00177-01
7a4b8e80938334aa2a110bb84e89c5da1efa59600cf29f932cdb2db66fa9305b	2CMV21-00177-01
84a2ab7e7d6f5a7d187a1159e2909b8a9086c1817fa840860e2a57f09d4341ad	2CMV21-00177-01
8c3684a7dc88ad3cf2b3c29d8152261a5c789a7ed5f8919286b695b07cd77269	2CMV21-00177-01
8d5486082fb6fab10930248f1ceaed46fa925b2b6802a390e7f20ffeb4b15933	2CMV21-00177-01
8ed83c8536661245ba55437b2edb44a51d7e16af475707e66bd216b4a2e3d417	2CMV21-00177-01
97504149a8582911df7c6da3a4c26b438375c83bd3a63240d4db69d7dffb6677	2CMV21-00177-01
9b8f3f6b8e389634d20861cbe272440c72797b5e2693f3ede9be1f3c230490a7	2CMV21-00177-01
9b9bff894fdf75c1647d96471aae20cc82bd183efbdfa2f06fe89c508df4fd58	2CMV21-00177-01
a3bccf3df83602916173c71787764bbfbae0a2b38825c35b63e14b67f734ff87	2CMV21-00177-01

a6bbdbebc8ceaa6ad1135b681b8fd27b8cd2a8b3c7a109bacdc9a7adb8619f61	2CMV21-00177-01
a9e803bd83a21e9205515f82a570aa90852bf4b56b6ababc42ca11158bc1c30c	2CMV21-00177-01
aa8fa2a4c86461f40755f3d7878a8b539b0f67086faeb12ff1c3d32f4369e0d1	2CMV21-00177-01
b608a010b1def6ecd045f448da9dba9773f793956ec28074333e310e89be3f1d	2CMV21-00177-01
c275e272a2c7c5d54227eddf82bdbee7efe52e1cd020765419943f49b5ad676b	2CMV21-00177-01
c7a345ed10dc3c955a39746257adeea524adb8e23dd1861830a8feafe737a431	2CMV21-00177-01
c7f6b747410720e04ce24be4781570754eccd3987ff554c191da350fd66149d8	2CMV21-00177-01
d086e1ce1ab085cd376dfe3aa210d940366a7375a5fb022f23d868ee03d876cd	2CMV21-00177-01
d608c0a3dbc66aa83df93a9ed831068cefb38f20fb9506e2bcdfe3fc1e1f2102	2CMV21-00177-01
df60968df156a0cd13104efb7b195ce95ab74ab6c1131f448751a5fe1cd184aa	2CMV21-00177-01
e0d5e245a3ea2bcc1be28c8ebcdbf42003bf72a382d60dfbf13f4c8302133df9	2CMV21-00177-01
eb59f4d9b291fcaf793cc20205de39a7b64e5f9674d3b9f2cd2c09d2ecdd5ef2	2CMV21-00177-01
ef6465de7408fb3a33634ac1e58ee57a3315e7a3f80b92fa5b00b622fbae104e	2CMV21-00177-01
f1a7ec16059aca15ee2f6c3eecc1094e20e06fceb658dcd5ed712f3f5613a18b	2CMV21-00177-01
fe7dd0ce1c21da4d16d00794634a7944a6357e4d768868192238c43057e20192	2CMV21-00177-01
a33d4b647cd9a415a96aa0aaa97bbaf2abf2817cf5eef4faf812a3216e9d1a9e	2CMV21-00177-01
2827c303dbc7117678703a2f6953bae8f6b23beb83810bc1433c6bc69e546bf9	2CMV21-00178-01
2148c99687b0f5a029a7a46cd198dea916d1e7919335b8b466051a871ac337a8	2CMV21-00178-01
77c503d69534472200c15546da7b8105754f852972293906e81a2783637c7a01	2CMV21-00178-01
ae6f8c9c11bba7d0ce66f3560ceb6fa1d9b3ca9dfa9e2973aec4f35ef0c81bbf	2CMV21-00178-01
3455bbf5c89bbcd3078370b9d8bae6481641921bd8ef4fa0bf251ffb609b3f63	2CMV21-00178-01
77c503d69534472200c15546da7b8105754f852972293906e81a2783637c7a01	2CMV21-00178-01
69a548be3eb238030389f288b6ba01536847ec9963e72fedcd2fabe32c5cdac2	2CMV21-00178-01
a41fe043906bfb0e06e822e12041333036d33463083aa049a9b1b982c5eb8664	2CMV21-00178-01
e3c91af6c6c0d3c1f82d3966eeaf30a8a10feae88388eb927610b37c0b505641	2CMV21-00178-01
b64bd75e963bb15686bbc134e1a9b432f196225d691e3dba30a414c80d6e318d	2CMV21-00178-01
e063675744fe156acc34f1eb72c72c2141cb362f19b7cc0d079a28fb4264d309	2CMV21-00178-01
0b279e2806a45a24a7d6a3cde92bc217a7b0f33e9b8279597594138ca5a6deb1	2CMV21-00178-01
51b0a60ce83bfd8ba1192241349594c0c3656898969ba79812bc67770be19184	2CMV21-00178-01
0f6bd7fd000a893d3f4680aa100e2e8f71796300a6102f8c5a84a04784a2fd0d	2CMV21-00178-01
9252454570564e20e58047b5eea3cffa8bdad7c1c837207e68b2688dbf859866	2CMV21-00178-01
95c81ec34aa4b87507aa0c92b9293d023637eac9f78f5562fc34bfa55c6b8a84	2CMV21-00178-01
1c348027f380cf209f7e6355762444f48e1f1d5f0ffb5d773ca2ddabd01fbf46	2CMV21-00178-01
160c99141a635337803c9f1ce56b6f8451601305228ef9348999ae96171e2546	2CMV21-00178-01
c5d2725c0c89273e5b92d370f269a48a37c481f0eb51e67dd731973c2409a039	2CMV21-00178-01
c5d2725c0c89273e5b92d370f269a48a37c481f0eb51e67dd731973c2409a039	2CMV21-00178-01
524207c70e8ef4601e4610b0cab735f3dd90275d4770f78da58c48b9a0d5786f	2CMV21-00178-01
54c52915b9a166cc18f39c86d2052699397ae13bd68b2e920d99c05edb17e836	2CMV21-00178-01

63259e2314404506e0e89981b847b7176122c5273116b7b7314c7ef989fb8a49	2CMV21-00178-01
e3155913ae30b127bff7ff81691758809791fb388b08a532a2541d2569fec5db	2CMV21-00178-01
17bba42544f3a1192ca0b2204350484e502c235b1a64c6825491181afb0893e8	2CMV21-00178-01
030c446ac1fac992dadf50c3926a07f9135232b6fbb0eda2ac40701d355567cd	2CMV21-00178-01
382befbed146b2655525f8c05d3c5a424d4b581c4160574ad8a0e37af6a59117	2CMV21-00178-01
e90a75c6c0f309cadcefdc757e524d60f582d8fb6bdb8d1a5579543836544bd7	2CMV21-00179-01
71ef7ae0787033b8a5a6a58f7a40fde476bb17d6547ded6a9d1a3b59d2d1a5c9	2CMV21-00179-01
b44a7254923b4fe76feef73eac203d4a910977cb1937148c49d4954c4bc6e9bc	2CMV21-00179-01
af303f91415b608a35352a7592e3f0925adfbf4623e1b9c392bc9f7bc5c99249	2CMV21-00179-01
137912378044bc3ba4510b1cb83960af13de376eafe5685b5502aab12c8fd938	2CMV21-00179-01
3ccf509d7e3a7233efe1ea866710ac47443a52018b5f522e698eab705b66ae77	2CMV21-00179-01
8b905bb18ae1914938e0efa93b6cf76ccb93f9c8fc2e46341d49e35fb4984a94	2CMV21-00179-01
fad5baa6211268a49e738df931a6e96b379afad4f72b98326d3e722566185f36	2CMV21-00179-01
8a4d0603f8b38ab69a0b4ed56703a866474ccc261c1930a6a9e93135404448e6	2CMV21-00179-01
81e70d32a66647a2e54e237662e6e5622f7208f12a6a50aa226d51741b9b4108	2CMV21-00179-01
e78f8edd92f050cc4338ce8439178f2c4a991dba47708d1eedbcb6c4c74681f6	2CMV21-00179-01
3c5d3b7b3899f6f566d8a8d614a90d46de31402689055cc3f89ba0826c57b2f4	2CMV21-00179-01
7be7c4a884cadbd072841ef05b2be3a71cedf0baf090578c895c3c4e2ad33288	2CMV21-00179-01
d921c052d7db250a55b471a682e71c4c9e7e390a287ab3962fbe364f596313e5	2CMV21-00179-01
3bf01c5858c2df2aeed82e57e8a3a8628b53462979e1c7adebfb571e2b00724c	2CMV21-00179-01
07fb3d4c094be965572a1801f9fa7117ae8d1cc7a2e60fb177a0a7571490a19e	2CMV21-00179-01
e012340a999d06f3b62b3a4553c15fe0c6e52a8f30a47b411b8cc29d9fdcb7d5	2CMV21-00179-01
64e0e69bbd7fe6dc1e89696e8cb677578f6e294bb7864f35ad1846444c559e90	2CMV21-00179-01
700f8fbfccf9cca6954b3278a9e210c74d2130cbac34e9cb75434ba95c0325d8	2CMV21-00179-01
902c8825330359fc1101a1b7c6e37d9a787bef981f43517c8c59673f4409284f	2CMV21-00179-01
6e9848539a1b357b306b12831ff163a2176318544282d09c9d0dfa1006810906	2CMV21-00179-01
5ad267f10b9a1a6112c24544085ce6b6e0952e21e038030b6c716a3d89551ae4	2CMV21-00179-01
0c2fb9c96823d0da59d80ab284317ccc78f485fed12792ded7c11105499dd4c0	2CMV21-00179-01
16197632c358c540d003a41a9c86b15bc7c5f62f59c0d0a78ac1f119759740c4	2CMV21-00179-01
dc9b22e3bb1ce4cdb2fb182bd3d0438d8ac8d087f8071fda96da900353a2feb3	2CMV21-00179-01
1d90143b37f1a3665a02790993a0e0ed27579e8618cc7d2236997af0c1d78e73	2CMV21-00179-01
7d37a477c968932fe9f9fb05399df3b984d2fd5c5900950c0118fa49dab90a40	2CMV21-00179-01
24b9f122349006afe996eb49534f12789789e56b5ebea1c4cae476ee13c0ce25	2CMV21-00179-01
04129eea5d80dbb823624e3b4f8c50d3a2ef628e0ac14f9518ee4dd8ae1ac9d1	2CMV21-00179-01
81c71c8981e51ce2f5c7e91082e309e5f51f73c2d87a57bd66e3abc48216f6d5	2CMV21-00179-01
a57864f7fe6f50a837cc246607931dd2bfeb6eeddadff285d02c4376df976329	2CMV21-00179-01
48f1aa8518644aea131ecb986aa3afcc51c0bd6d2273486fe2424fc88c3edcd1	2CMV21-00179-01
cbc87d70317d1e6ae7b31e7b04aaf4d4f3657fa547366b39bc8553d8e25544a6	2CMV21-00179-01

30089f814f88d498a179e73e00bcf7c5fc56b9fbe29e3b4ae935236d33535b90	2CMV21-00179-01
9289affcd05962100d36f8af38249cb43ac1938f862853527e9bb54c26e58d6c	2CMV21-00179-01
05e335ea50465d760f277ca8593ac29777d4a01b31f282bd559d2c151d73903c	2CMV21-00179-01
80f1a2a50f44cac7a53ca43499cba6fa828f754f26ea4903e17f855db8d492ba	2CMV21-00179-01
41d0e5e67449f4f8bdce0b17cda2352a69484e2141840fe7aa7853364f945398	2CMV21-00179-01
e07c9bb4ff74d295bb8efd69ad48f4cb519dcc6ae97e05e22621a5e946f2cd68	2CMV21-00179-01
ee04202f0840eb7a24c85313cbdd18e70080d130d237a8ee9900f46662d63a15	2CMV21-00179-01
d66f236820b0811b68c09210632814279653a744080e4a906407a982e7be83fa	2CMV21-00179-01
12bb4a69f7164e88e17f92821fd40d3ef7712f7e6a541f2f49c74ba64225b995	2CMV21-00179-01
27a7100d87ce7101a0312999c7e7868ad8d44a7f7354cf7e2ac17bd9e8d25381	2CMV21-00179-01
4e7e4999a14414d17794db24864f29e04ee3dae35867909b1c7060f54d4e04ee	2CMV21-00179-01
c1dff9ee3990040bc2897b6833ac8664e7a9cae109ff44dff2c4a106563cf53b	2CMV21-00179-01

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
220.84.103.2	Korea Telecom	2CMV21-00177-01
1.209.16.178	LG DACOM Corporation	2CMV21-00177-01
185.222.57.148	bd-rootlayer-1-mnt	2CMV21-00177-01
200.152.105.190	MLS Projetos de Informatica	2CMV21-00177-01
157.90.122.246	RIPE Network Coordination Centre	2CMV21-00177-01
188.165.179.11	AVIRAHOST S.C Servidores	2CMV21-00177-01
75.127.1.107	ColoCrossing	2CMV21-00177-01
46.183.221.107	DataClub S.A.	2CMV21-00177-01
185.222.58.157	bd-rootlayer-1-mnt	2CMV21-00177-01
185.222.57.134	bd-rootlayer-1-mnt	2CMV21-00177-01
125.214.169.206	Dialog Axiata Plc	2CMV21-00177-01
103.68.183.3	Better Cloud Limited	2CMV21-00177-01
177.131.10.152	Data Info Comercio e Servico Ltda.	2CMV21-00177-01
209.133.223.107	NOC4Hosts Inc.	2CMV21-00177-01
104.129.30.165	QuadraNet Enterprises LLC	2CMV21-00177-01
209.127.16.116	B2 Net Solutions Inc.	2CMV21-00177-01
74.198.0.41	Rogers Communications Canada Inc.	2CMV21-00177-01
103.114.107.198	Son Thuy Investment Trading and Service Company Limited	2CMV21-00177-01

1.209.188.135	LG DACOM Corporation	2CMV21-00177-01
205.147.111.56	Asia Pacific Network Information Centre	2CMV21-00177-01
103.245.209.153	AS Data(Hong Kong)Limited	2CMV21-00177-01
51.255.128.81	Ghiaci Erfan	2CMV21-00177-01
51.254.77.49	Perva Ciprian	2CMV21-00177-01
95.63.48.1	Infraestructura Red y Servicios IP	2CMV21-00177-01
192.241.151.27	DigitalOcean LLC	2CMV21-00177-01
45.160.79.229	Wan Developments S.A.S	2CMV21-00177-01
72.188.127.223	Charter Communications Inc	2CMV21-00177-01
206.189.17.54	DigitalOcean LLC	2CMV21-00177-01
186.250.40.29	REDE MINAS TELECOM LTDA	2CMV21-00177-01
31.210.21.71	Des Capital B.V.	2CMV21-00178-01
84.38.129.16	DataClub S.A.	2CMV21-00178-01
45.87.60.140	Hyonix LLC	2CMV21-00178-01
46.183.221.120	DataClub S.A.	2CMV21-00178-01
64.188.20.220	QUADRANET-GLOBAL	2CMV21-00178-01
77.247.110.104	ABC Consultancy	2CMV21-00178-01
45.144.225.194	Des Capital B.V.	2CMV21-00178-01
45.137.22.37	RootLayer Web Services Ltd	2CMV21-00178-01
185.29.8.26	DataClub S.A.	2CMV21-00178-01
45.137.22.67	RootLayer Web Services Ltd.	2CMV21-00178-01
103.155.80.223	VIETNAM POSTS AND TELECOMMUNICATIONS GROUP	2CMV21-00178-01
77.247.110.220	ABC Consultancy	2CMV21-00178-01
172.93.160.141	QUADRANET-GLOBAL	2CMV21-00178-01
104.129.30.165	QUADRANET-GLOBAL	2CMV21-00178-01
88.198.99.168	Hetzner Online GmbH	2CMV21-00178-01
189.206.78.79	Alestra S. de R.L. de C.V.	2CMV21-00179-01
201.130.73.237	Mexico Red de Telecomunicaciones S. de R.L. de C.V.	2CMV21-00179-01
178.128.26.199	digitalocean	2CMV21-00179-01
112.169.6.253	Korea Telecom	2CMV21-00179-01
186.64.123.128	ZAM LTDA.	2CMV21-00179-01
182.16.1.139	SIMCENTRIC-HK NETBLOCK	2CMV21-00179-01
86.135.38.47	IP pools	2CMV21-00179-01
138.34.78.8	ETA Technologies Corporation	2CMV21-00179-01
45.63.93.254	The Constant Company LLC	2CMV21-00179-01
192.30.243.240	Majestic Hosting Solutions LLC	2CMV21-00179-01
47.180.237.125	Frontier Communications Corporation	2CMV21-00179-01
200.252.0.67	Ivel Acre Veï¿½culos LTDA	2CMV21-00179-01

103.221.49.110	Shanghai Kuanhui Tech. Co. Ltd	2CMV21-00179-01
128.14.152.198	Zenlayer Inc	2CMV21-00179-01
124.198.82.6	HAIonNet	2CMV21-00179-01
96.67.25.153	Comcast Cable Communications LLC	2CMV21-00179-01
177.223.252.212	THS Provider Servicos de Comunicacao Multimidia LT	2CMV21-00179-01
66.45.148.88	Midcontinent Communications	2CMV21-00179-01
148.251.210.176	RIPE Network Coordination Centre	2CMV21-00179-01
5.39.125.250	jalil abdul	2CMV21-00179-01
45.15.10.59	Teleglobal Communication Services Limited	2CMV21-00179-01
185.121.120.179	Serverion BV	2CMV21-00179-01
103.232.53.68	VietServer Services technology company limited	2CMV21-00179-01
103.139.44.182	Trung Hieu Services Trading Investment Company Limited	2CMV21-00179-01
151.236.52.249	RIPE Network Coordination Centre	2CMV21-00179-01
103.114.107.198	Son Thuy Investment Trading and Service Company Limited	2CMV21-00179-01
172.93.123.140	Host4Geeks LLC	2CMV21-00179-01
62.75.206.159	PlusServer GmbH	2CMV21-00179-01
80.122.5.54	360grad gmbh	2CMV21-00179-01
185.222.57.143	bd-rootlayer-1-mnt	2CMV21-00179-01
185.222.57.148	bd-rootlayer-1-mnt	2CMV21-00179-01
103.138.69.195	PT. Internetwork Komunikasi Indonesia	2CMV21-00179-01
185.222.57.188	bd-rootlayer-1-mnt	2CMV21-00179-01

Actualidad

Ciberconsejos | Qué son las Amenazas Persistentes Avanzadas y cómo protegernos

Logran permanecer en los sistemas de sus víctimas, sin ser detectados, por largo tiempo. E incluso si su infección principal es erradicada, se las ingenian para dejar una puerta abierta en el sistema y regresar con fuerza. Los actores maliciosos pueden lograr esto gracias a las Amenazas Persistentes Avanzadas (APT), y en el CSIRT de Gobierno preparamos estos ciberconsejos para que conocerlas y poder estar mejor protegidos ante ellas.

Encuentra la infografía completa en PDF, aquí: https://www.csirt.gob.cl/media/2021/05/Landing-Amenazas-Persistentes-Avanzadas-2.pdf


Ministerio del Interior y Seguridad Pública
CSIRT
CIBERCONSEJOS DE SEGURIDAD
AMENAZAS PERSISTENTES AVANZADAS (APT)
CARACTERÍSTICAS
MANTENER el entorno TI con evaluación de vulnerabilidades y gestión eficiente de parches
ELIMINAR privilegios administrativos locales de las cuentas en estaciones de trabajo de los usuarios y limitar su acceso a lo necesario
DESARROLLAR pruebas de penetración y ejercicios prácticos de simulación de ataques que emulan actores APT
GENERAR conciencia de estos riesgos en la organización para formar estrategias de defensa eficaces
Ministerio del Interior y Seguridad Pública
CSIRT
CIBERCONSEJOS DE SEGURIDAD
AMENAZAS PERSISTENTES AVANZADAS (APT)
RECOMENDACIONES
IDENTIFICAR todos los activos tecnológicos que componen el alcance a defender
DESARROLLAR arquitecturas de redes y sistemas que contemplen medidas de ciberseguridad avanzadas
IMPLEMENTAR una correcta estrategia de registro y monitoreo de "logs"
ESTABLECER un plan de comunicaciones que ayude a los usuarios a comprender las amenazas y cómo identificarlas

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.

- Christian Campodónico
- Pablo Ascencio
- Eduardo Riveros

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2021.05.20 12:09:52 -04'00'