Alerta de seguridad informática	8FFR-00123-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 de Noviembre de 2019
Última revisión	24 de Noviembre de 2019

NOTIFICACIÓN

La información consignada en el presente informe es producto del análisis de múltiples fuentes, de terceras partes e investigación propia del equipo CSIRT. La información contenida en los informes o comunicados está afecta a actualizaciones, por lo cual se recomienda establecer una cuarentena preventiva respecto de los IoC mencionados, previa evaluación de impacto en servicios productivos; una vez que sus plataformas de monitoreo no detecten actividad maliciosa, se debe evaluar la posibilidad de liberar del bloqueo a los IoC consignados en el reporte respectivo, tales como servicios de hosting, de cloud o similares.

Estos casos de fraude no involucran directamente a las entidades ni al sistema bancario, sino que son técnicas de fraude indirecto, en las que en infraestructura externa a éstas se arma el mencionado fraude, para construir el engaño. Las entidades, en general, al tomar conocimiento de estos portales maliciosos articulan, dentro de sus potestades y marco legal vigente, las acciones necesarias para poder desarticularlos, pero ciertamente los usuarios también estamos llamados a estar atentos a estos intentos de engaño.

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de un portal fraudulento asociado a una IP que suplanta el sitio web oficial de **Banco Estado**, el que podría servir para robar credenciales de usuarios de esa entidad.

Lo anterior constituye una falsificación de la marca institucional que podría afectar a usuarios, clientes y a la entidad bancaria aludida.

Indicadores de Compromisos

URL´s

URL Sitio Clonado:
https[://]6y3zelqlstbiutogfjgf9q-on[.]drv[.]tw/bncstado1/index_2[.]html

nationaldisabilitylawyer[.]com/libraries/www[.]bancoestado[.]cl/

http[://]www[.]carpetworldlondon[.]com/cmfchile/imagenes/comun2008/banca-en-linea-personas[.]html

Domain drv.tw

drv / tw / Subdomains

record type	TTL	value		
A	1799	47.254.47.165		
A	1799	47.89.250.243		
NS	1800	freedns2.registrar-servers.com	Zones on DNS server	104.216.69.250
NS	1800	freedns3.registrar-servers.com	Zones on DNS server	195.154.94.174
NS	1800	freedns4.registrar-servers.com	Zones on DNS server	95.141.37.127
NS	1800	freedns1.registrar-servers.com	Zones on DNS server	45.58.122.82
NS	1800	freedns5.registrar-servers.com	Zones on DNS server	54.36.109.15
TXT	1799	google-site-verification=pg6v4yKk9duvrnGAkYiO_q9-J9DN6V3KVmlL1Ia2osU		
SOA	3601	Mname: freedns1.registrar-servers.com Rname: hostmaster.registrar-servers.com Serial number: 2019102900 Refresh: 43200 Retry: 3600 Expire: 604800 Minimum TTL: 3601		

Domain nationaldisabilitylawyer.com

nationaldisabilitylawyer / com / Subdomains

record type	TTL	value		
A	14400	162.241.226.115		
NS	86400	ns2.bluehost.com	Zones on DNS server	162.159.25.175
NS	86400	ns1.bluehost.com	Zones on DNS server	162.159.24.80
MX	14400	0 nationaldisabilitylawyer.com		
TXT	14400	v=spf1 a mx ptr include:bluehost.com ?all		
SOA	86400	Mname: ns1.bluehost.com Rname: dnsadmin.box5340.bluehost.com Serial number: 2017110107 Refresh: 86400 Retry: 7200 Expire: 3600000 Minimum TTL: 300		

Domain www.carpetworldlondon.com

www / carpetworldlondon / com / Subdomains

record type	TTL	value	
CNAME	14400	carpetworldlondon.com	148.72.23.31

Ilustración 1 Dominio donde se Aloja Url del Banco Estado, Falso y DNS que utiliza

Certificados

Criteria Identity = 'drv.tw'; Exclude expired certificates

Certificates

crt.sh ID	Logged At	Not Before	Not After	Issuer Name
1987580530	2019-10-10	2019-10-10	2020-01-08	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1979967640	2019-10-10	2019-10-10	2020-01-08	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3

Criteria Identity = 'nationaldisabilitylawyer.com'

Certificates

crt.sh ID	Logged At	Not Before	Not After	Issuer Name
2002523179	2019-10-15	2019-10-15	2020-01-13	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
2002102377	2019-10-15	2019-10-15	2020-01-13	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1781157244	2019-08-14	2019-08-14	2019-11-12	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1772036808	2019-08-14	2019-08-14	2019-11-12	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1583517904	2019-06-14	2019-06-14	2019-09-12	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1576761117	2019-06-14	2019-06-14	2019-09-12	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1390531801	2019-04-14	2019-04-14	2019-07-13	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1385202800	2019-04-14	2019-04-14	2019-07-13	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1197576554	2019-02-12	2019-02-12	2019-05-13	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1195333918	2019-02-12	2019-02-12	2019-05-13	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1024515099	2018-12-12	2018-12-12	2019-03-12	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1024514655	2018-12-12	2018-12-12	2019-03-12	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
854075119	2018-10-12	2018-10-12	2019-01-10	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
854218488	2018-10-12	2018-10-12	2019-01-10	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
739393579	2018-08-12	2018-08-12	2018-11-10	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
672655832	2018-08-12	2018-08-12	2018-11-10	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
521672284	2018-06-12	2018-06-12	2018-09-10	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
521628285	2018-06-12	2018-06-12	2018-09-10	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3

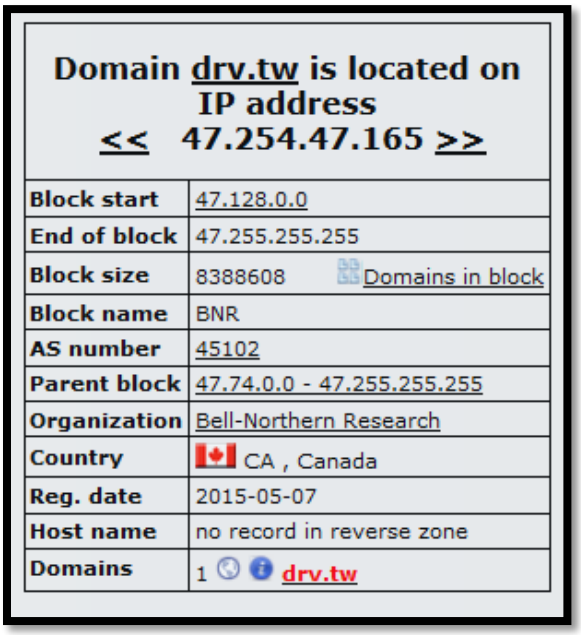
Criteria Identity = 'www.carpetworldlondon.com'

Certificates

crt.sh ID	Logged At	Not Before	Not After	Issuer Name
2040991160	2019-10-27	2019-10-27	2020-01-25	C=US, ST=TX, L=Houston, O="cPanel, Inc.", CN="cPanel, Inc. Certification Authority"
2040990747	2019-10-27	2019-10-27	2020-01-25	C=US, ST=TX, L=Houston, O="cPanel, Inc.", CN="cPanel, Inc. Certification Authority"
1853258788	2019-09-06	2019-09-06	2019-12-05	C=US, ST=TX, L=Houston, O="cPanel, Inc.", CN="cPanel, Inc. Certification Authority"
1853258533	2019-09-06	2019-09-06	2019-12-05	C=US, ST=TX, L=Houston, O="cPanel, Inc.", CN="cPanel, Inc. Certification Authority"
1780699877	2019-08-17	2019-08-17	2019-11-15	C=US, ST=TX, L=Houston, O="cPanel, Inc.", CN="cPanel, Inc. Certification Authority"
1780699641	2019-08-17	2019-08-17	2019-11-15	C=US, ST=TX, L=Houston, O="cPanel, Inc.", CN="cPanel, Inc. Certification Authority"
1484596284	2019-05-18	2019-05-18	2019-08-16	C=US, ST=TX, L=Houston, O="cPanel, Inc.", CN="cPanel, Inc. Certification Authority"
1484594018	2019-05-18	2019-05-18	2019-08-16	C=US, ST=TX, L=Houston, O="cPanel, Inc.", CN="cPanel, Inc. Certification Authority"
1484137242	2019-05-18	2019-05-18	2019-08-16	C=US, ST=TX, L=Houston, O="cPanel, Inc.", CN="cPanel, Inc. Certification Authority"
1484135086	2019-05-18	2019-05-18	2019-08-16	C=US, ST=TX, L=Houston, O="cPanel, Inc.", CN="cPanel, Inc. Certification Authority"
1250432097	2019-03-03	2019-03-03	2019-06-01	C=US, ST=TX, L=Houston, O="cPanel, Inc.", CN="cPanel, Inc. Certification Authority"
1250432193	2019-03-03	2019-03-03	2019-06-01	C=US, ST=TX, L=Houston, O="cPanel, Inc.", CN="cPanel, Inc. Certification Authority"
1035929957	2018-12-17	2018-12-17	2019-03-17	C=US, ST=TX, L=Houston, O="cPanel, Inc.", CN="cPanel, Inc. Certification Authority"
1035934511	2018-12-17	2018-12-17	2019-03-17	C=US, ST=TX, L=Houston, O="cPanel, Inc.", CN="cPanel, Inc. Certification Authority"
996345378	2018-12-03	2018-12-03	2019-03-03	C=US, ST=TX, L=Houston, O="cPanel, Inc.", CN="cPanel, Inc. Certification Authority"
996344884	2018-12-03	2018-12-03	2019-03-03	C=US, ST=TX, L=Houston, O="cPanel, Inc.", CN="cPanel, Inc. Certification Authority"
762755857	2018-09-18	2018-09-18	2018-12-17	C=US, ST=TX, L=Houston, O="cPanel, Inc.", CN="cPanel, Inc. Certification Authority"
762754722	2018-09-18	2018-09-18	2018-12-17	C=US, ST=TX, L=Houston, O="cPanel, Inc.", CN="cPanel, Inc. Certification Authority"
671613916	2018-08-05	2018-08-05	2018-11-03	C=US, ST=TX, L=Houston, O="cPanel, Inc.", CN="cPanel, Inc. Certification Authority"
671613093	2018-08-05	2018-08-05	2018-11-03	C=US, ST=TX, L=Houston, O="cPanel, Inc.", CN="cPanel, Inc. Certification Authority"

Ilustración 2 Certificado Utilizado en Url del sitio Falso del Banco Estado

IP
47.254.47.165
162.241.226.115
148.72.23.31



Domain drv.tw is located on IP address
<< 47.254.47.165 >>

Block start	47.128.0.0
End of block	47.255.255.255
Block size	8388608 Domains in block
Block name	BNR
AS number	45102
Parent block	47.74.0.0 - 47.255.255.255
Organization	Bell-Northern Research
Country	CA , Canada
Reg. date	2015-05-07
Host name	no record in reverse zone
Domains	1 drv.tw

Domain nationaldisabilitylawyer.com is located on IP address
<< 162.241.226.115 >>

Block start	162.240.0.0
End of block	162.241.255.255
Block size	131072 Domains in block
Block name	UNIFIEDLAYER-NETWORK-16
AS number	46606
Parent block	162.0.0.0 - 162.255.255.255
Organization	UnifiedLayer
City	Provo
Region/State	Utah
Country	US , United States
Reg. date	2013-08-22
Host name	box5340.bluehost.com

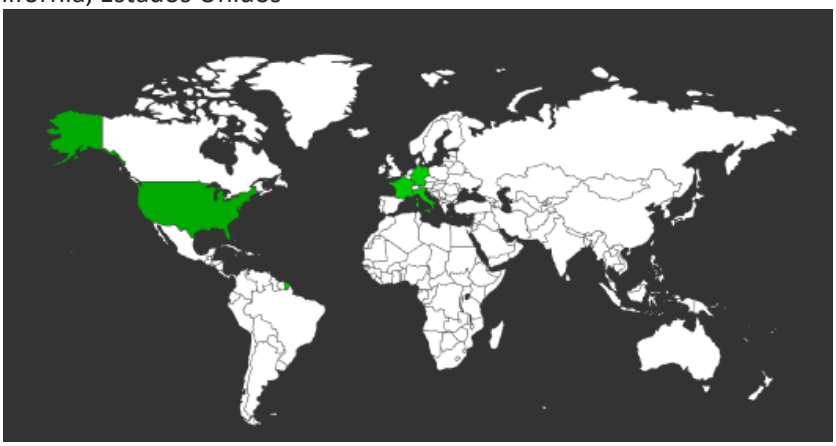
Domain www.carpetworldlondon.com is located on IP address << 148.72.23.31 >>

Block start	148.69.0.0
End of block	148.73.255.255
Block size	327680 Domains in block
Block name	SPACENET-SPAN
AS number	26496
Parent block	148.69.0.0 - 148.78.255.255
Organization	Spacenet, Inc.
City	Scottsdale
Region/State	Arizona
Country	US , United States
Reg. date	1991-04-11
Host name	ip-148-72-23-31.ip.secureserver.net
Domains	1 www.carpetworldlondon.com

Ilustración 3 Ip de Origen donde se aloja Sitio Falso del Banco Estado

Localización

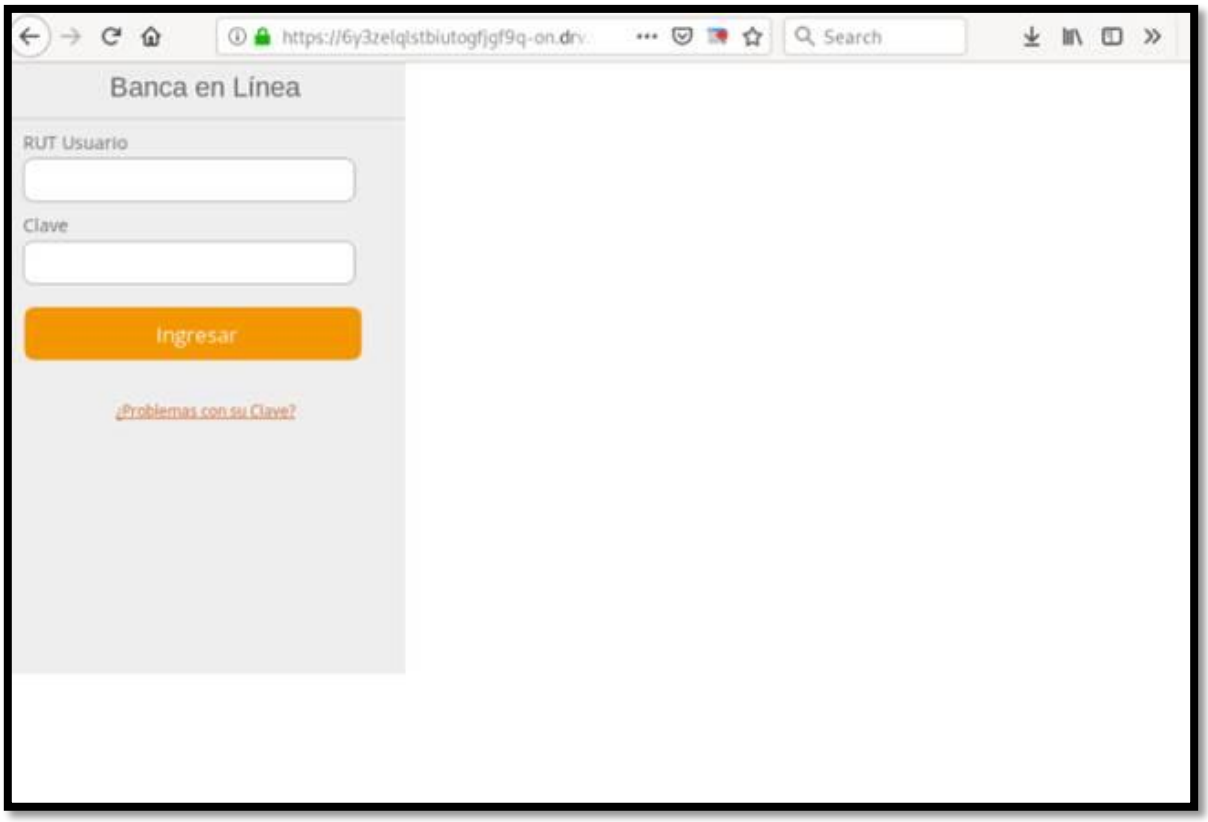
San Mateo, California, Estados Unidos

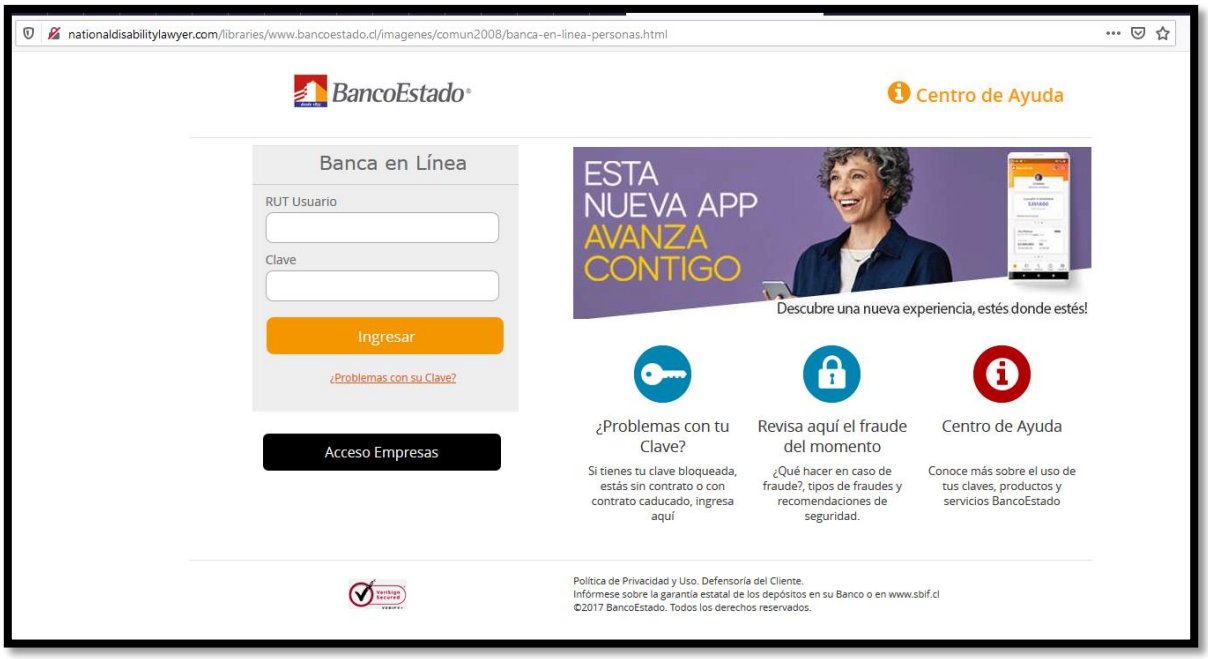


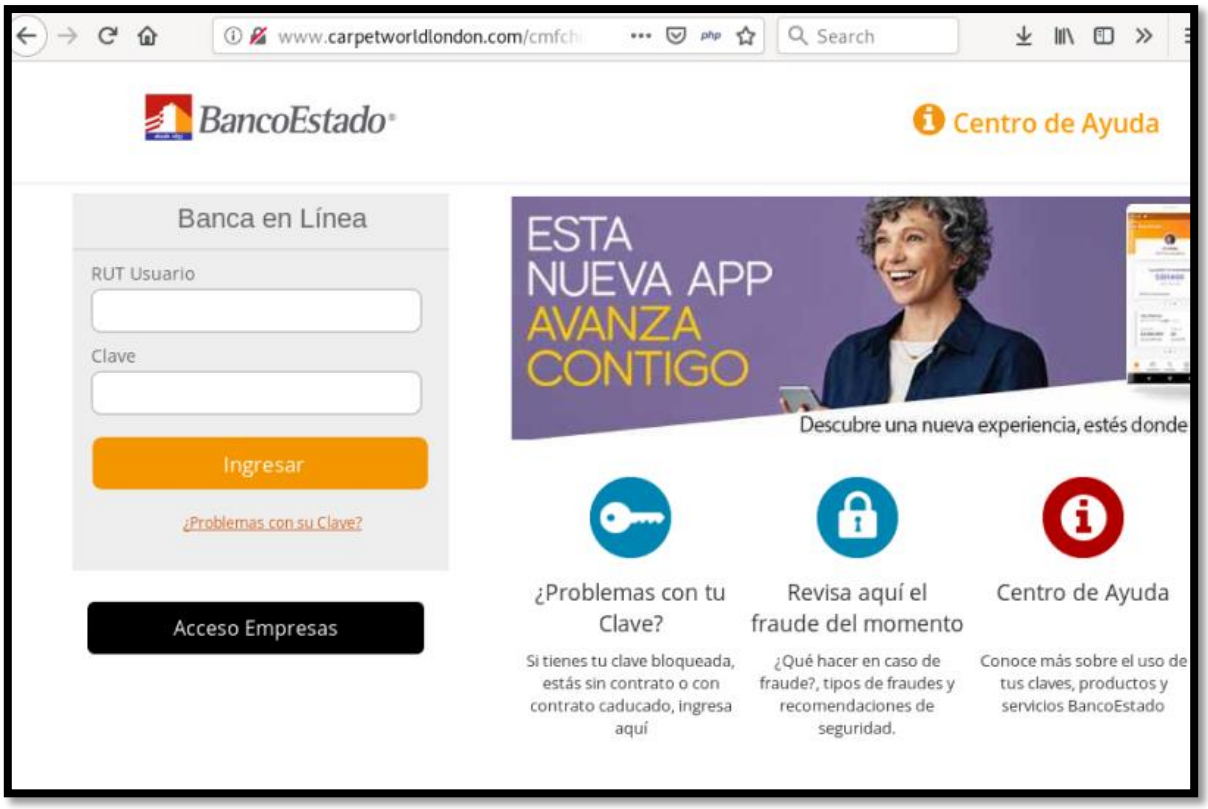
Provo, Utah, Estados Unidos

Scottsdale, Arizona, Estados Unidos

Imagen del sitio






www.carpetworldlondon.com/cmfch
Search
BancoEstado
Centro de Ayuda
Banca en Línea
RUT Usuario
Clave
Ingresar
¿Problemas con su Clave?
Acceso Empresas
ESTA NUEVA APP AVANZA CONTIGO
Descubre una nueva experiencia, estés donde
¿Problemas con tu Clave?
Si tienes tu clave bloqueada, estás sin contrato o con contrato caducado, ingresa aquí
Revisa aquí el fraude del momento
¿Qué hacer en caso de fraude?, tipos de fraudes y recomendaciones de seguridad.
Centro de Ayuda
Conoce más sobre el uso de tus claves, productos y servicios BancoEstado

Whois

```
% IANA WHOIS server
% for more information on IANA, visit http://www.iana.org
% This query returned 1 object

refer:        whois.twnic.net.tw

domain:       TW

organisation: Taiwan Network Information Center (TWNIC)
address:      4F-2, No. 9, Roosevelt Road, Section 2
address:      Taipei  100
address:      Taiwan

contact:      administrative
name:         Vice CEO
organisation: Taiwan Network Information Center (TWNIC)
address:      4F-2, No. 9, Roosevelt Road, Section 2
address:      Taipei  100
address:      Taiwan
phone:        +886 2 2341 1313 ext. 126
fax-no:       +886 2 2396 8832
e-mail:       tw-admin@twnic.tw

contact:      technical
name:         Director of Technical Department
organisation: Taiwan Network Information Center (TWNIC)
address:      4F-2, No. 9, Roosevelt Road, Section 2
address:      Taipei  100
address:      Taiwan
phone:        +886 2 2341-1313 ext. 500
fax-no:       +886 2 2396-8832
e-mail:       tech-admin@twnic.tw

nserver:      A.DNS.TW 2001:45b1:0:5:0:0:0:25 203.73.24.25
nserver:      ANYTLD.APNIC.NET 2001:dd8:12:0:0:0:0:53 202.12.31.53
nserver:      B.DNS.TW 210.201.138.58 2404:0:10a0:0:0:0:0:58
nserver:      C.DNS.TW 2001:b020:0:77:0:0:0:1 203.66.87.201
nserver:      D.DNS.TW 2001:4541:9010:7:0:0:0:186 60.199.165.186
nserver:      E.DNS.TW 2001:b000:1e0:c000:0:0:0:11 211.20.231.11
nserver:      F.DNS.TW 163.28.1.10
nserver:      G.DNS.TW 2001:cd8:400:0:0:0:0:195 220.229.225.195
nserver:      H.DNS.TW 2001:500:14:6119:ad:0:0:1 204.61.216.119
nserver:      NS.TWNIC.NET 192.83.166.11 2001:288:1:1006:0:0:0:11
ds-rdata:     40792 8 2 A05DB4B0DEB97103136lBB621E8BB1B8D7346665A3D1B06EC1431ADB7D015EE9

whois:        whois.twnic.net.tw

status:       ACTIVE
remarks:      Registration information: http://rs.twnic.net.tw

created:      1989-07-31
changed:      2019-01-15
source:       IANA

Domain Name: drv.tw

   Contact:
      Anny Miser
      drvtw@outlook.com


   Record expires on 2021-12-20 (YYYY-MM-DD)
```

```
Domain Name: NATIONALDISABILITYLAWYER.COM
Registry Domain ID: 135658312_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.networksolutions.com
Registrar URL: http://networksolutions.com
Updated Date: 2018-09-24T07:55:56Z
Creation Date: 2004-11-23T05:43:35Z
Registrar Registration Expiration Date: 2021-11-23T05:43:35Z
Registrar: Network Solutions, LLC
Registrar IANA ID: 2
Reseller:
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Registry Registrant ID:
Registrant Name: PERFECT PRIVACY, LLC
Registrant Organization:
Registrant Street: 5335 Gate Parkway care of Network Solutions PO Box 459
Registrant City: Jacksonville
Registrant State/Province: FL
Registrant Postal Code: 32256
Registrant Country: US
Registrant Phone: +1.5707088780
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: rd9pw5vt2w2@networksolutionsprivateregistration.com
Registry Admin ID:
Admin Name: PERFECT PRIVACY, LLC
Admin Organization:
Admin Street: 5335 Gate Parkway care of Network Solutions PO Box 459
Admin City: Jacksonville
Admin State/Province: FL
Admin Postal Code: 32256
Admin Country: US
Admin Phone: +1.5707088780
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: rd9pw5vt2w2@networksolutionsprivateregistration.com
Registry Tech ID:
Tech Name: PERFECT PRIVACY, LLC
Tech Organization:
Tech Street: 5335 Gate Parkway care of Network Solutions PO Box 459
Tech City: Jacksonville
Tech State/Province: FL
Tech Postal Code: 32256
Tech Country: US
Tech Phone: +1.5707088780
Tech Phone Ext:
Tech Fax:
Tech Fax Ext:
Tech Email: rd9pw5vt2w2@networksolutionsprivateregistration.com
Name Server: NS1.BLUEHOST.COM
Name Server: NS2.BLUEHOST.COM
DNSSEC: unsigned
Registrar Abuse Contact Email: abuse@web.com
Registrar Abuse Contact Phone: +1.8003337680
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2019-11-20T13:58:21Z <<<
```

```
Domain Name: carpetworldlondon.com
Registry Domain ID: 1939814249_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: http://www.godaddy.com
Updated Date: 2019-06-15T04:03:26Z
Creation Date: 2015-06-18T10:36:47Z
Registrar Registration Expiration Date: 2021-06-18T10:36:47Z
Registrar: GoDaddy.com, LLC
Registrar IANA ID: 146
Registrar Abuse Contact Email: abuse@godaddy.com
Registrar Abuse Contact Phone: +1.4806242505
Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited http://www.icann.org/epp#clientUpdateProhibited
Domain Status: clientRenewProhibited http://www.icann.org/epp#clientRenewProhibited
Domain Status: clientDeleteProhibited http://www.icann.org/epp#clientDeleteProhibited
Registrant Organization: Sharp Professional Services Ltd
Registrant State/Province: Middlesex
Registrant Country: UK
Registrant Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=carpetworldlondon.com
Admin Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=carpetworldlondon.com
Tech Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=carpetworldlondon.com
Name Server: NS46.CARPETWORLDLONDON.COM
Name Server: NS47.CARPETWORLDLONDON.COM
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2019-11-20T15:00:00Z <<<
```

Recomendaciones

- Evitar acceder al sitio anteriormente indicado e informar a los usuarios sobre su existencia, para evitar que se conviertan en víctimas del fraude.
- Ser precavidos frente a este tipo de páginas fraudulentas.
- Bloquear en los proxy o sistemas de control de contenido, hacia la URL maliciosa
- 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

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2019.11.24 08:25:03 -03'00'