Alerta de seguridad informática	8FFR20-00260-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 de Marzo de 2020
Última revisión	13 de Marzo de 2020

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 tres portales fraudulentos asociados a tres IP que suplantan el sitio web oficial de Banco Scotiabank, 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

www1[.]scotia[.]chileweb[.]cl[.]int01[.]online
www1[.]scotia[.]chileweb[.]cl[.]nel01[.]online
www-scotia-web-portal-personas-chile[.]cl[.]fsnursing[.]com/89DZFM/login/I7Y3R/personas//

Domain www1.scotia.chileweb.cl.int01.online

www1 / scotia / chileweb / cl / int01 / online / Subdomains

record type	TTL	value
A	7207	139.59.70.252

Domain int01.online

int01 / online / Subdomains

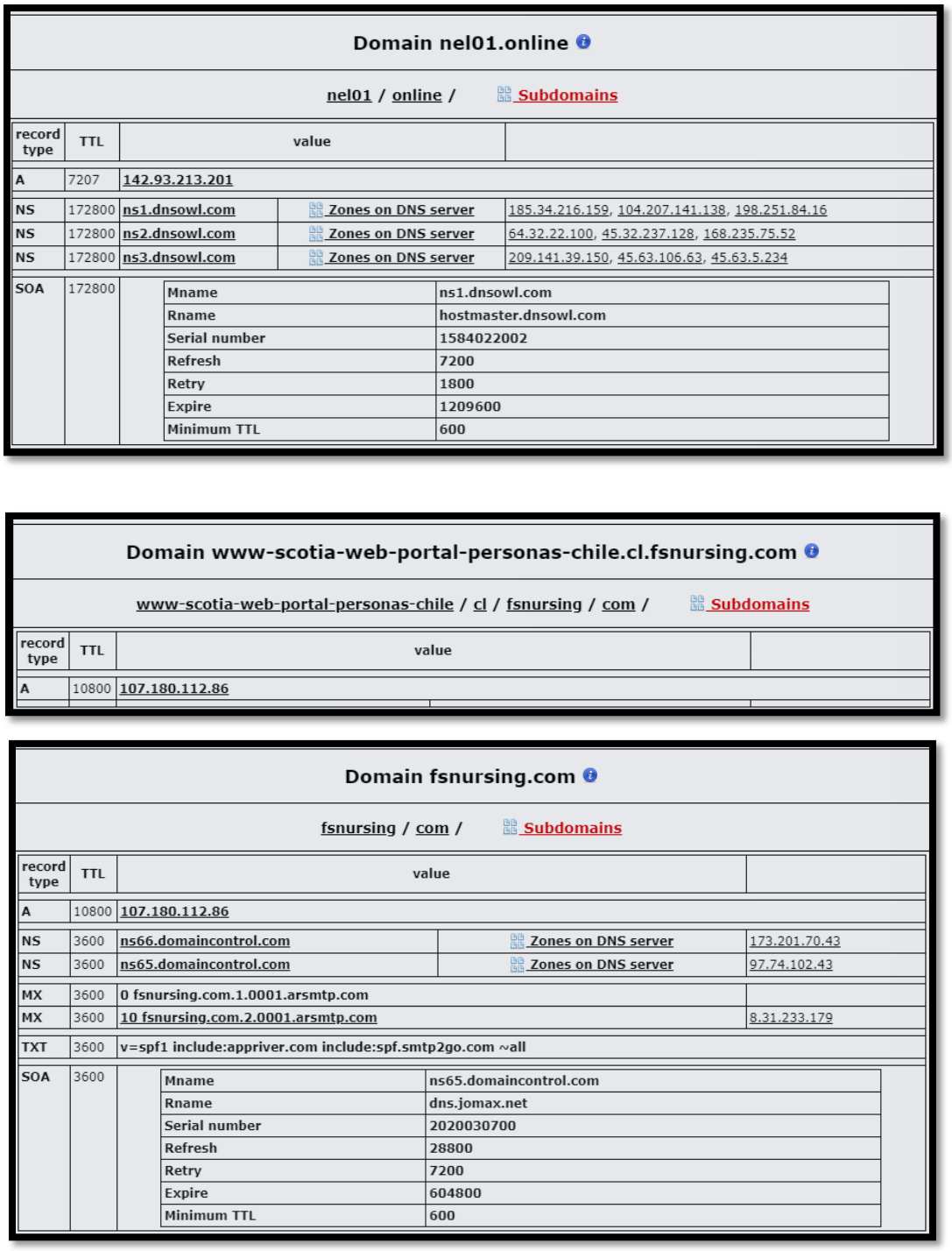
record type	TTL	value		
A	7207	139.59.70.252		
NS	172800	ns1.dnsowl.com	Zones on DNS server	185.34.216.159, 104.207.141.138, 198.251.84.16
NS	172800	ns2.dnsowl.com	Zones on DNS server	64.32.22.100, 45.32.237.128, 168.235.75.52
NS	172800	ns3.dnsowl.com	Zones on DNS server	45.63.5.234, 209.141.39.150, 45.63.106.63

SOA	172800	Mname	ns1.dnsowl.com
		Rname	hostmaster.dnsowl.com
		Serial number	1584022002
		Refresh	7200
		Retry	1800
		Expire	1209600
		Minimum TTL	600

Domain www1.scotia.chileweb.cl.nel01.online

www1 / scotia / chileweb / cl / nel01 / online / Subdomains

record type	TTL	value
A	7207	142.93.213.201



Domain nel01.online

nel01 / online / Subdomains

record type	TTL	value		
A	7207	142.93.213.201		
NS	172800	ns1.dnsowl.com	Zones on DNS server	185.34.216.159, 104.207.141.138, 198.251.84.16
NS	172800	ns2.dnsowl.com	Zones on DNS server	64.32.22.100, 45.32.237.128, 168.235.75.52
NS	172800	ns3.dnsowl.com	Zones on DNS server	209.141.39.150, 45.63.106.63, 45.63.5.234

SOA	172800	Mname	ns1.dnsowl.com
		Rname	hostmaster.dnsowl.com
		Serial number	1584022002
		Refresh	7200
		Retry	1800
		Expire	1209600
		Minimum TTL	600

Domain www-scotia-web-portal-personas-chile.cl.fsnursing.com

www-scotia-web-portal-personas-chile / cl / fsnursing / com / Subdomains

record type	TTL	value
A	10800	107.180.112.86

Domain fsnursing.com

fsnursing / com / Subdomains

record type	TTL	value		
A	10800	107.180.112.86		
NS	3600	ns66.domaincontrol.com	Zones on DNS server	173.201.70.43
NS	3600	ns65.domaincontrol.com	Zones on DNS server	97.74.102.43
MX	3600	0 fsnursing.com.1.0001.arsmtp.com		
MX	3600	10 fsnursing.com.2.0001.arsmtp.com		8.31.233.179
TXT	3600	v=spf1 include:appriver.com include:spf.smtp2go.com ~all		

SOA	3600	Mname	ns65.domaincontrol.com
		Rname	dns.jomax.net
		Serial number	2020030700
		Refresh	28800
		Retry	7200
		Expire	604800
		Minimum TTL	600

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

Certificados

Certificates

crt.sh ID	Logged At	Not Before	Not After	Matching Identities	Issuer Name
2566688333	2020-03-11	2020-03-11	2020-06-09	www1.scotia.chileweb.cl.int01.online	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3

Certificates

crt.sh ID	Logged At	Not Before	Not After	Matching Identities	Issuer Name
2566341294	2020-03-11	2020-03-11	2020-06-09	www1.scotia.chileweb.cl.nel01.online	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3

Certificates

crt.sh ID	Logged At	Not Before	Not After	Matching Identities	Issuer Name
2564442908	2020-03-07	2020-03-07	2020-06-05	www-scotia-web-portal-personas-chile.cl.fsnursing.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
2550240174	2020-03-07	2020-03-07	2020-06-05	www-scotia-web-portal-personas-chile.cl.fsnursing.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3

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

IP

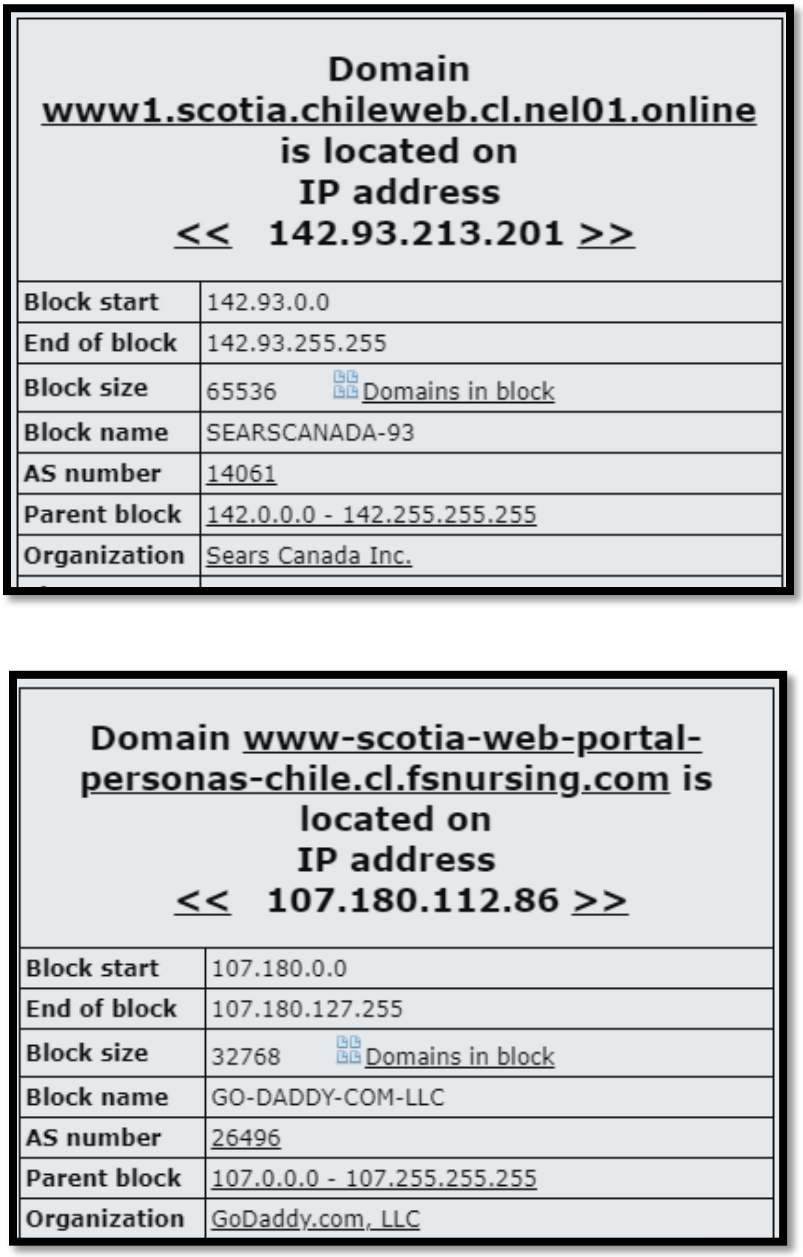
139[.]59[.]70[.]252

142[.]93[.]213[.]201

107[.]180[.]112[.]86

Domain www1.scotia.chileweb.cl.int01.online is located on IP address << 139.59.70.252 >>

Block start	139.59.0.0
End of block	139.59.255.254
Block size	65535 Domains in block
Block name	DIGITALOCEAN-AP
AS number	14061
Parent block	139.59.0.0 - 139.59.255.255
Organization	DigitalOcean, LLC



Domain www1.scotia.chileweb.cl.nel01.online is located on IP address << 142.93.213.201 >>

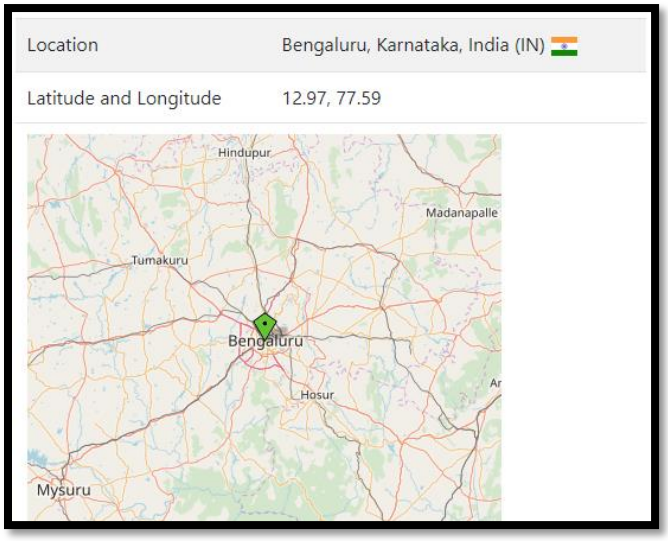
Block start	142.93.0.0
End of block	142.93.255.255
Block size	65536 Domains in block
Block name	SEARSCANADA-93
AS number	14061
Parent block	142.0.0.0 - 142.255.255.255
Organization	Sears Canada Inc.

Domain www-scotia-web-portal-personas-chile.cl.fsnursing.com is located on IP address << 107.180.112.86 >>

Block start	107.180.0.0
End of block	107.180.127.255
Block size	32768 Domains in block
Block name	GO-DADDY-COM-LLC
AS number	26496
Parent block	107.0.0.0 - 107.255.255.255
Organization	GoDaddy.com, LLC

Ilustración 2 Ip de Origen donde se aloja Sitio Falso del Banco Scotiabank

Localización
Bengaluru, Karnataka, India
New York City, New York, Estados Unidos



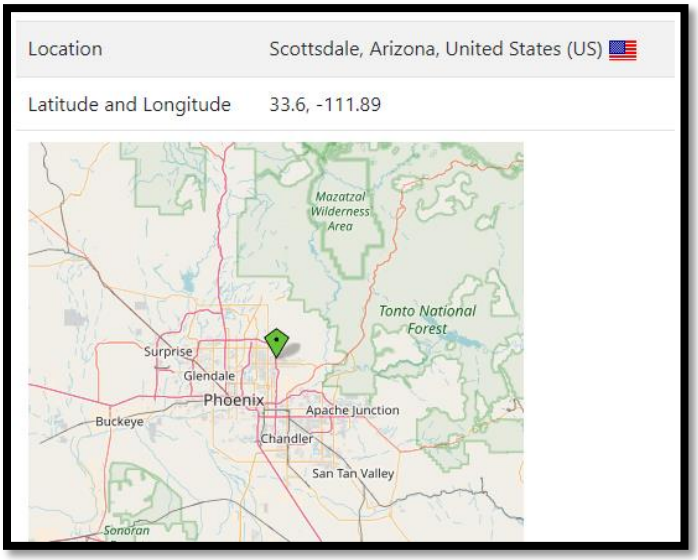
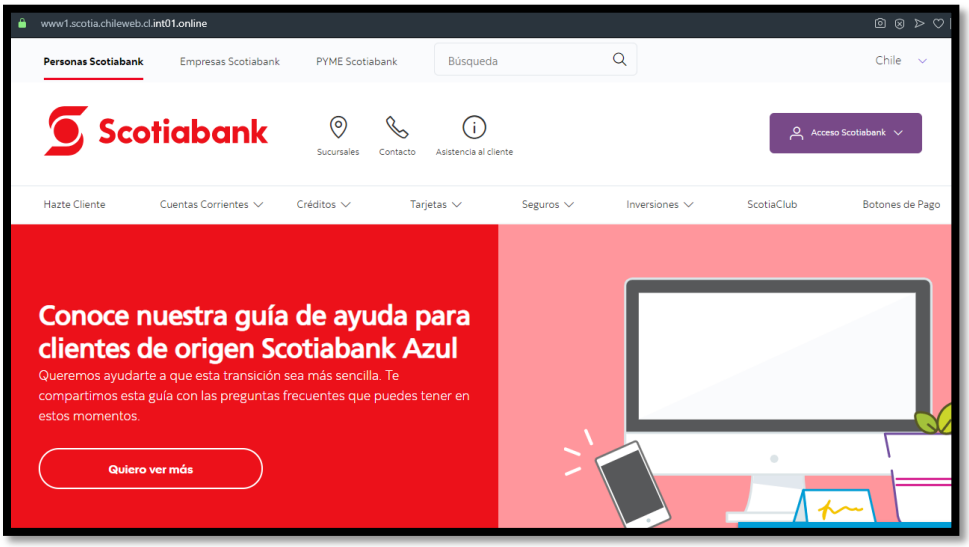
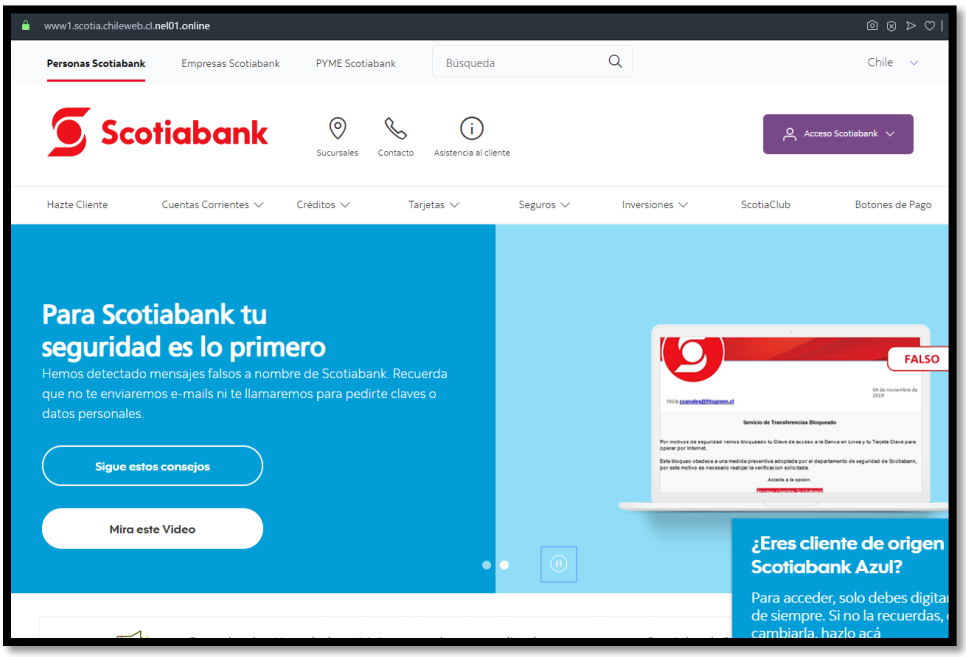
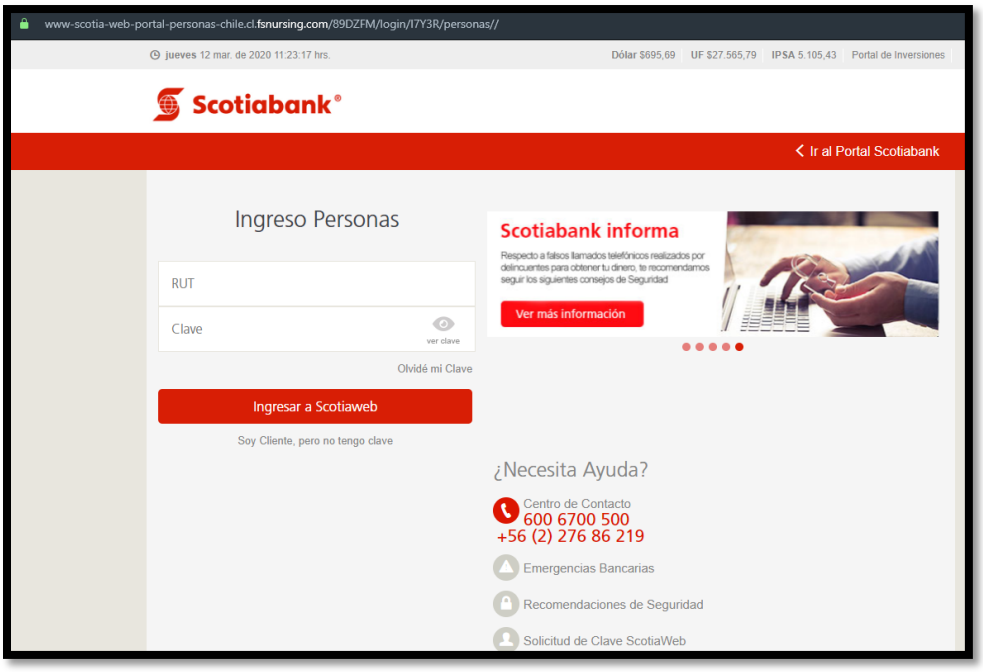


Imagen del sitio






www-scotia-web-portal-personas-chile.cl.fsnursing.com/89DZFM/login/I7Y3R/personas//
jueves 12 mar. de 2020 11:23:17 hrs.
Dólar $695,69
UF $27.565,79
IPSA 5.105,43
Portal de Inversiones
Scotiabank
Ir al Portal Scotiabank
Ingreso Personas
RUT
Clave
ver clave
Olvidé mi Clave
Ingresar a Scotiaweb
Soy Cliente, pero no tengo clave
Scotiabank informa
Respecto a falsos llamados telefónicos realizados por delincuantes para obtener tu dinero, te recomendamos seguir los siguientes consejos de Seguridad
Ver más información
¿Necesita Ayuda?
Centro de Contacto
600 6700 500
+56 (2) 276 86 219
Emergencias Bancarias
Recomendaciones de Seguridad
Solicitud de Clave ScotiaWeb

Whois

```
Domain Name: int01.online
Registry Domain ID: D177504959-CNIC
Registrar WHOIS Server: whois.namesilo.com
Registrar URL: https://www.namesilo.com/
Updated Date: 2020-03-11T07:00:00Z
Creation Date: 2020-03-10T07:00:00Z
Registrar Registration Expiration Date: 2021-03-11T07:00:00Z
Registrar: NameSilo, LLC
Registrar IANA ID: 1479
Registrar Abuse Contact Email: abuse@namesilo.com
Registrar Abuse Contact Phone: +1.4805240066
Domain Status: clientTransferProhibited https://www.icann.org/epp#clientTransferProhibited
Registry Registrant ID:
Registrant Name: Domain Administrator
Registrant Organization: See PrivacyGuardian.org
Registrant Street: 1928 E. Highland Ave. Ste F104 PMB# 255
Registrant City: Phoenix
Registrant State/Province: AZ
Registrant Postal Code: 85016
Registrant Country: US
Registrant Phone: +1.3478717726
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: pw-17fbf81096c31e44d1f962c230f523b1@privacyguardian.org
Registry Admin ID:
Admin Name: Domain Administrator
Admin Organization: See PrivacyGuardian.org
Admin Street: 1928 E. Highland Ave. Ste F104 PMB# 255
Admin City: Phoenix
Admin State/Province: AZ
Admin Postal Code: 85016
Admin Country: US
Admin Phone: +1.3478717726
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: pw-17fbf81096c31e44d1f962c230f523b1@privacyguardian.org
Registry Tech ID:
Tech Name: Domain Administrator
Tech Organization: See PrivacyGuardian.org
Tech Street: 1928 E. Highland Ave. Ste F104 PMB# 255
Tech City: Phoenix
Tech State/Province: AZ
Tech Postal Code: 85016
Tech Country: US
Tech Phone: +1.3478717726
Tech Phone Ext:
Tech Fax:
Tech Fax Ext:
Tech Email: pw-17fbf81096c31e44d1f962c230f523b1@privacyguardian.org
Name Server: NS1.DNSOWL.COM
Name Server: NS2.DNSOWL.COM
Name Server: NS3.DNSOWL.COM
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2020-03-12T07:00:00Z <<<
```

```
Domain Name: nel01.online
Registry Domain ID: D178421464-CNIC
Registrar WHOIS Server: whois.namesilo.com
Registrar URL: https://www.namesilo.com/
Updated Date: 2020-03-12T07:00:00Z
Creation Date: 2020-03-11T07:00:00Z
Registrar Registration Expiration Date: 2021-03-11T07:00:00Z
Registrar: NameSilo, LLC
Registrar IANA ID: 1479
Registrar Abuse Contact Email: abuse@namesilo.com
Registrar Abuse Contact Phone: +1.4805240066
Domain Status: clientTransferProhibited https://www.icann.org/epp#clientTransferProhibited
Registry Registrant ID:
Registrant Name: Domain Administrator
Registrant Organization: See PrivacyGuardian.org
Registrant Street: 1928 E. Highland Ave. Ste F104 PMB# 255
Registrant City: Phoenix
Registrant State/Province: AZ
Registrant Postal Code: 85016
Registrant Country: US
Registrant Phone: +1.3478717726
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: pw-9135dll5d3f6f2f3ad6c9275fcld0c6c@privacyguardian.org
Registry Admin ID:
Admin Name: Domain Administrator
Admin Organization: See PrivacyGuardian.org
Admin Street: 1928 E. Highland Ave. Ste F104 PMB# 255
Admin City: Phoenix
Admin State/Province: AZ
Admin Postal Code: 85016
Admin Country: US
Admin Phone: +1.3478717726
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: pw-9135dll5d3f6f2f3ad6c9275fcld0c6c@privacyguardian.org
Registry Tech ID:
Tech Name: Domain Administrator
Tech Organization: See PrivacyGuardian.org
Tech Street: 1928 E. Highland Ave. Ste F104 PMB# 255
Tech City: Phoenix
Tech State/Province: AZ
Tech Postal Code: 85016
Tech Country: US
Tech Phone: +1.3478717726
Tech Phone Ext:
Tech Fax:
Tech Fax Ext:
Tech Email: pw-9135dll5d3f6f2f3ad6c9275fcld0c6c@privacyguardian.org
Name Server: NS1.DNSOWL.COM
Name Server: NS2.DNSOWL.COM
Name Server: NS3.DNSOWL.COM
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2020-03-12T07:00:00Z <<<
```

```
Domain Name: fsnursing.com
Registry Domain ID: 1988551805_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: http://www.godaddy.com
Updated Date: 2019-12-21T11:21:35Z
Creation Date: 2015-12-20T17:20:36Z
Registrar Registration Expiration Date: 2020-12-20T17:20:36Z
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:
Registrant State/Province: NY
Registrant Country: US
Registrant Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=fsnursing.com
Admin Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=fsnursing.com
Tech Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=fsnursing.com
Name Server: NS65.DOMAINCONTROL.COM
Name Server: NS66.DOMAINCONTROL.COM
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2020-03-12T14:00:00Z <<<

For more information on Whois status codes, please visit https://www.icann.org/resources/pages/epp-status-codes-2014-06-16-
en

Notes:

IMPORTANT: Port43 will provide the ICANN-required minimum data set per
ICANN Temporary Specification, adopted 17 May 2018.
Visit https://whois.godaddy.com to look up contact data for domains
not covered by GDPR policy.

The data contained in GoDaddy.com, LLC's WhoIs database,
while believed by the company to be reliable, is provided "as is"
with no guarantee or warranties regarding its accuracy.  This
information is provided for the sole purpose of assisting you
in obtaining information about domain name registration records.
Any use of this data for any other purpose is expressly forbidden without the prior written
permission of GoDaddy.com, LLC.  By submitting an inquiry,
you agree to these terms of usage and limitations of warranty.  In particular,
you agree not to use this data to allow, enable, or otherwise make possible,
dissemination or collection of this data, in part or in its entirety, for any
purpose, such as the transmission of unsolicited advertising and
and solicitations of any kind, including spam.  You further agree
not to use this data to enable high volume, automated or robotic electronic
processes designed to collect or compile this data for any purpose,
including mining this data for your own personal or commercial purposes.

Please note: the registrant of the domain name is specified
in the "registrant" section.  In most cases, GoDaddy.com, LLC
is not the registrant of domain names listed in this database.
```

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: 2020.03.13 09:54:38 -03'00'