Alerta de Seguridad Informática

Alerta de seguridad informática	8FFR20-00225-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	21 de Febrero de 2020
Última revisión	21 de Febrero de 2020

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de seis portales fraudulentos asociados a tres IP que suplantan el sitio web oficial del **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

URLs
scotia[.]chileweb[.]cl[.]0c1[.]live
www1[.]scotia[.]chileweb[.]cl[.]0c1[.]live
scotia[.]chileweb[.]cl[.]0c2[.]live
www2[.]scotia[.]chileweb[.]cl[.]0c2[.]live
scotia[.]chileweb[.]cl[.]0c3[.]live
www3[.]scotia[.]chileweb[.]cl[.]0c3[.]live

Domain 0c1.live

0c1 / live / Subdomains

record type	TTL	value		
A	7207	165.22.220.251		
NS	172800	ns1.dnsowl.com	Zones on DNS server	104.207.141.138, 198.251.84.16, 185.34.216.159
NS	172800	ns2.dnsowl.com	Zones on DNS server	64.32.22.100, 168.235.75.52, 45.32.237.128
NS	172800	ns3.dnsowl.com	Zones on DNS server	209.141.39.150, 45.63.5.234, 45.63.106.63
SOA	172800	Mname	ns1.dnsowl.com	
		Rname	hostmaster.dnsowl.com	
		Serial number	1582205788	
		Refresh	7200	
		Retry	1800	
		Expire	1209600	
		Minimum TTL	600	

Domain scotia.chileweb.cl.0c1.live

scotia / chileweb / cl / 0c1 / live / Subdomains

record type	TTL	value	
A	7207	165.22.220.251	

Domain 0c2.live

0c2 / live / Subdomains

record type	TTL	value		
A	7207	134.209.156.250		
NS	172800	ns1.dnsowl.com	Zones on DNS server	104.207.141.138, 198.251.84.16, 185.34.216.159
NS	172800	ns2.dnsowl.com	Zones on DNS server	45.32.237.128, 168.235.75.52, 64.32.22.100
NS	172800	ns3.dnsowl.com	Zones on DNS server	45.63.106.63, 45.63.5.234, 209.141.39.150
SOA	172800	Mname	ns1.dnsowl.com	
		Rname	hostmaster.dnsowl.com	
		Serial number	1582206685	
		Refresh	7200	
		Retry	1800	
		Expire	1209600	
		Minimum TTL	600	

Domain scotia.chileweb.cl.0c2.live

scotia / chileweb / cl / 0c2 / live / Subdomains

record type	TTL	value	
A	7207	134.209.156.250	

Domain 0c3.live

0c3 / live / Subdomains

record type	TTL	value		
A	7207	68.183.95.33		
NS	172800	ns1.dnsowl.com	Zones on DNS server	104.207.141.138, 198.251.84.16, 185.34.216.159
NS	172800	ns2.dnsowl.com	Zones on DNS server	45.32.237.128, 168.235.75.52, 64.32.22.100
NS	172800	ns3.dnsowl.com	Zones on DNS server	45.63.106.63, 45.63.5.234, 209.141.39.150
SOA	172800	Mname	ns1.dnsowl.com	
		Rname	hostmaster.dnsowl.com	
		Serial number	1582206685	
		Refresh	7200	
		Retry	1800	
		Expire	1209600	
		Minimum TTL	600	

Domain scotia.chileweb.cl.0c3.live

scotia / chileweb / cl / 0c3 / live / Subdomains

record type	TTL	value	
A	7207	68.183.95.33	

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

Certificados

Subject DN	CN=www1.scotia.chileweb.cl.0c1.live
Issuer DN	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
Serial	284492076477438760553814138441840581824431
Validity	2020-02-20 03:55:10 **to** 2020-05-20 03:55:10 (90 days, 0:00:00)
Names	www1.scotia.chileweb.cl.0c1.live

Subject DN	CN=www2.scotia.chileweb.cl.0c2.live
Issuer DN	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
Serial	310220530677946624268269198817371504330131
Validity	2020-02-20 03:55:55 **to** 2020-05-20 03:55:55 (90 days, 0:00:00)
Names	www2.scotia.chileweb.cl.0c2.live

Subject DN	CN=www3.scotia.chileweb.cl.0c3.live
Issuer DN	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
Serial	301307616750676437291815944191714635127281
Validity	2020-02-20 03:57:09 **to** 2020-05-20 03:57:09 (90 days, 0:00:00)
Names	www3.scotia.chileweb.cl.0c3.live

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

IP
165[.]22[.]220[.]251
134[.]209[.]156[.]250
68[.]183[.]95[.]33

Domain scotia.chileweb.cl.0c1.live is located on IP address
<< 165.22.220.251 >>

Block start	165.22.0.0
End of block	165.22.255.255
Block size	65536 Domains in block
Block name	CELTECH1
AS number	14061
Parent block	165.0.0.0 - 165.255.255.255
Organization	CellularTechnicalServices
City	Seattle
Region/State	Washington
Country	US , United States
Reg. date	1993-03-31
Host name	no record in reverse zone
Domains	1 scotia.chileweb.cl.0c1.live

Domain scotia.chileweb.cl.0c2.live is located on IP address << 134.209.156.250 >>

Block start	134.209.0.0
End of block	134.209.255.255
Block size	65536 Domains in block
Block name	COV-HC-NET134
AS number	14061
Parent block	134.0.0.0 - 134.255.255.255
Organization	COVIDIENLP
City	Mansfield
Region/State	Massachusetts
Country	US , United States
Reg. date	1989-07-24
Host name	no record in reverse zone
Domains	1 scotia.chileweb.cl.0c2.live

Domain scotia.chileweb.cl.0c3.live is located on IP address << 68.183.95.33 >>

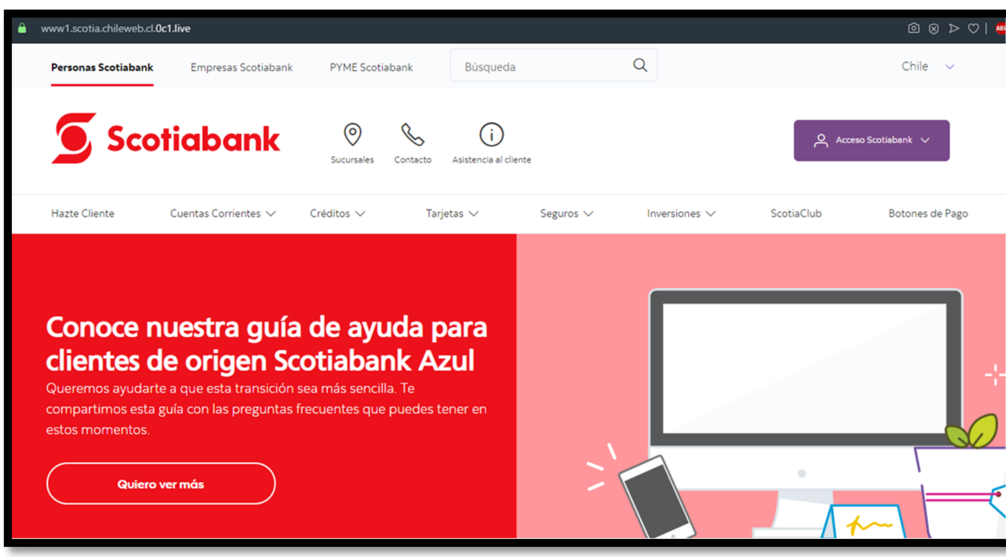
Block start	68.183.0.0
End of block	68.183.255.255
Block size	65536 Domains in block
Block name	DSLEXTREME-NWK-6
AS number	14061
Parent block	68.0.0.0 - 68.255.255.255
Organization	DSL Extreme
City	Chatsworth
Region/State	California
Country	US , United States
Reg. date	2005-04-14
Host name	no record in reverse zone
Domains	1 scotia.chileweb.cl.0c3.live

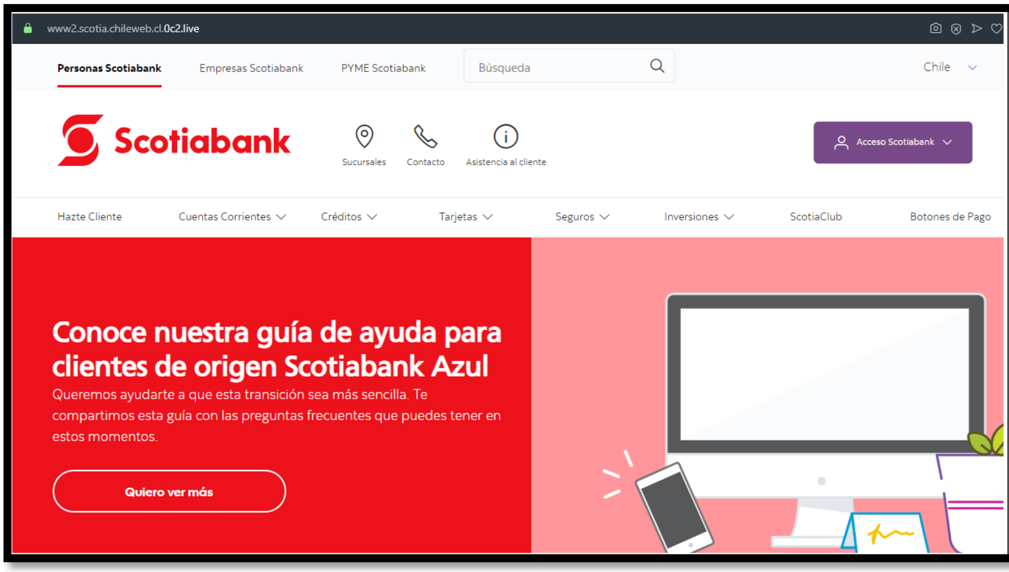
Ilustración 3 Ip de Origen donde se aloja Sitio Falso del Banco Scotiabank

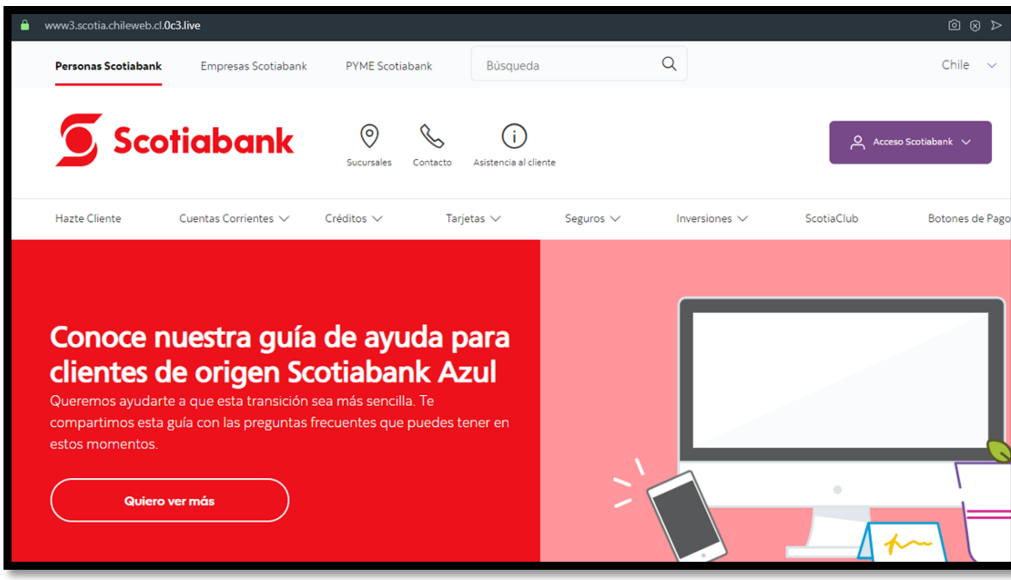
Localización

India, Bangalore, Karnataka

Imagen del sitio




www2.scotia.chileweb.cl.0c2.live
Personas Scotiabank
Empresas Scotiabank
PYME Scotiabank
Búsqueda
Chile
Scotiabank
Sucursales
Contacto
Asistencia al cliente
Acceso Scotiabank
Hazte Cliente
Cuentas Corrientes
Créditos
Tarjetas
Seguros
Inversiones
ScotiaClub
Botones de Pago
Conoce nuestra guía de ayuda para clientes de origen Scotiabank Azul
Queremos ayudarte a que esta transición sea más sencilla. Te compartimos esta guía con las preguntas frecuentes que puedes tener en estos momentos.
Quiero ver más


www3.scotia.chileweb.cl.0c3.live
Personas Scotiabank
Empresas Scotiabank
PYME Scotiabank
Búsqueda
Chile
Scotiabank
Sucursales
Contacto
Asistencia al cliente
Acceso Scotiabank
Hazte Cliente
Cuentas Corrientes
Créditos
Tarjetas
Seguros
Inversiones
ScotiaClub
Botones de Pago
Conoce nuestra guía de ayuda para clientes de origen Scotiabank Azul
Queremos ayudarte a que esta transición sea más sencilla. Te compartimos esta guía con las preguntas frecuentes que puedes tener en estos momentos.
Quiero ver más

Whois

```
Domain Name: 0c1.live
Registry Domain ID: eefb9800eba8493bb5991961847eaa71-DONUTS
Registrar WHOIS Server: whois.namesilo.com
Registrar URL: https://www.namesilo.com/
Updated Date: 2020-02-19T07:00:00Z
Creation Date: 2020-02-18T07:00:00Z
Registrar Registration Expiration Date: 2021-02-18T07:00:00Z
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#clientTra
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-7b6b8cab6a7602eaae8b5fbf0edd956d@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-7b6b8cab6a7602eaae8b5fbf0edd956d@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-7b6b8cab6a7602eaae8b5fbf0edd956d@privacyguardian.org
Name Server: NS1.DNSOWL.COM
Name Server: NS2.DNSOWL.COM
Name Server: NS3.DNSOWL.COM
DNSSEC: unsigned
```

```
Domain Name: 0c2.live
Registry Domain ID: a85c6d0302ec46a79301945a46c529a5-DONUTS
Registrar WHOIS Server: whois.namesilo.com
Registrar URL: https://www.namesilo.com/
Updated Date: 2020-02-19T07:00:00Z
Creation Date: 2020-02-18T07:00:00Z
Registrar Registration Expiration Date: 2021-02-18T07:00:00Z
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#clientTransferPro
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-04dbca9df82fab730bcaa1ed572d1006@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-04dbca9df82fab730bcaa1ed572d1006@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-04dbca9df82fab730bcaa1ed572d1006@privacyguardian.org
Name Server: NS1.DNSOWL.COM
Name Server: NS2.DNSOWL.COM
Name Server: NS3.DNSOWL.COM
DNSSEC: unsigned
```

```
Domain Name: 0c3.live
Registry Domain ID: e69bdb9e18ce46df9a289f5261e86bea-DONUTS
Registrar WHOIS Server: whois.namesilo.com
Registrar URL: https://www.namesilo.com/
Updated Date: 2020-02-19T07:00:00Z
Creation Date: 2020-02-18T07:00:00Z
Registrar Registration Expiration Date: 2021-02-18T07:00:00Z
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#clientTransferPr
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-7a008071ca62d51d94ff45d710475b2f@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-7a008071ca62d51d94ff45d710475b2f@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-7a008071ca62d51d94ff45d710475b2f@privacyguardian.org
Name Server: NS1.DNSOWL.COM
Name Server: NS2.DNSOWL.COM
Name Server: NS3.DNSOWL.COM
DNSSEC: unsigned
```

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: 2020.02.21 12:02:56 -03'00'