Alerta de seguridad informática	8FFR20-00220-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	18 de Febrero de 2020
Última revisión	18 de Febrero 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 dos 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.

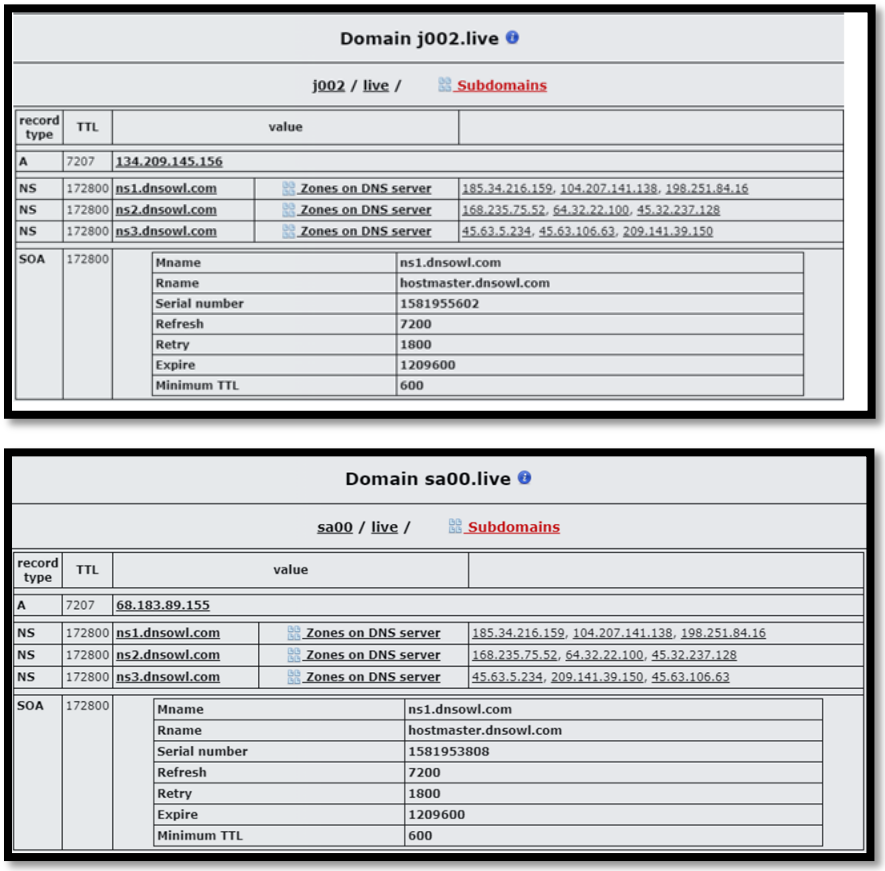
Indicadores de Compromisos

URLs

http://www3[.]scotia[.]chile[.]j002[.]live/

https://www2[.]scotia[.]chile[.]j002[.]live/

wws[.]scotia[.]chile[.]sa00[.]live/



Domain j002.live

j002 / live / Subdomains

record type	TTL	value		
A	7207	134.209.145.156		
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	168.235.75.52, 64.32.22.100, 45.32.237.128
NS	172800	ns3.dnsowl.com	Zones on DNS server	45.63.5.234, 45.63.106.63, 209.141.39.150
SOA	172800	Mname	ns1.dnsowl.com	
		Rname	hostmaster.dnsowl.com	
		Serial number	1581955602	
		Refresh	7200	
		Retry	1800	
		Expire	1209600	
		Minimum TTL	600	

Domain sa00.live

sa00 / live / Subdomains

record type	TTL	value		
A	7207	68.183.89.155		
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	168.235.75.52, 64.32.22.100, 45.32.237.128
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	1581953808	
		Refresh	7200	
		Retry	1800	
		Expire	1209600	
		Minimum TTL	600	

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

Certificados

Subject DN	CN=www2.scotia.chile.j002.live
Issuer DN	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
Serial	304198026347325112420750529719770713707604
Validity	2020-02-15 04:51:12 **to** 2020-05-15 04:51:12 (90 days, 0:00:00)
Names	www2.scotia.chile.j002.live

Subject DN	CN=wws.scotia.chile.sa00.live
Issuer DN	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
Serial	302908909118848870733921706304527370347094
Validity	2020-02-15 04:49:23 **to** 2020-05-15 04:49:23 (90 days, 0:00:00)
Names	wws.scotia.chile.sa00.live

Certificado

Subject DN	CN=www2.scotia.chile.j002.live
Issuer DN	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
Serial	304198026347325112420750529719770713707604
Validity	2020-02-15 04:51:12 **to** 2020-05-15 04:51:12 (90 days, 0:00:00)
Names	www2.scotia.chile.j002.live

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

IP

134[.]209[.]145[.]156
68[.]183[.]89[.]155

Network information

IP address	134.209.145.156
Reverse DNS (PTR record)	not available
DNS server (NS record)	ns2.digitalocean.com (173.245.59.41) ns3.digitalocean.com (198.41.222.173) ns1.digitalocean.com (173.245.58.51)
ASN number	14061
ASN name (ISP)	DigitalOcean, LLC
IP-range/subnet	134.209.144.0/20 134.209.144.0 - 134.209.159.255

IP Lookup Results for:

68.183.89.155

IP	68.183.89.155	**ASN No.**	14061

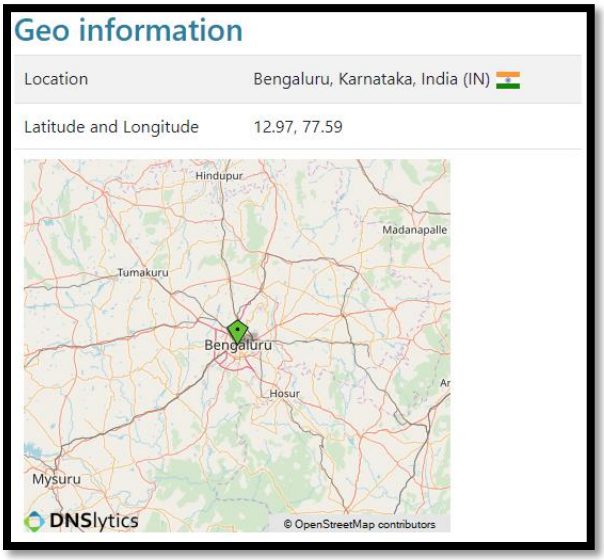
IP Location via DB-IP (PRODUCT: API, REAL-TIME)

City	Coimbatore	**State**	Tamil Nadu	**Country**	India
ISP	DigitalOcean, LLC	**Latitude**	11.0056	**Longitude**	76.9661
Organization	DSL Extreme	**Is proxy**	NO	**Is crawler**	NO
Threat Level	low				

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

Localización

Bangalore, Karnataka, India



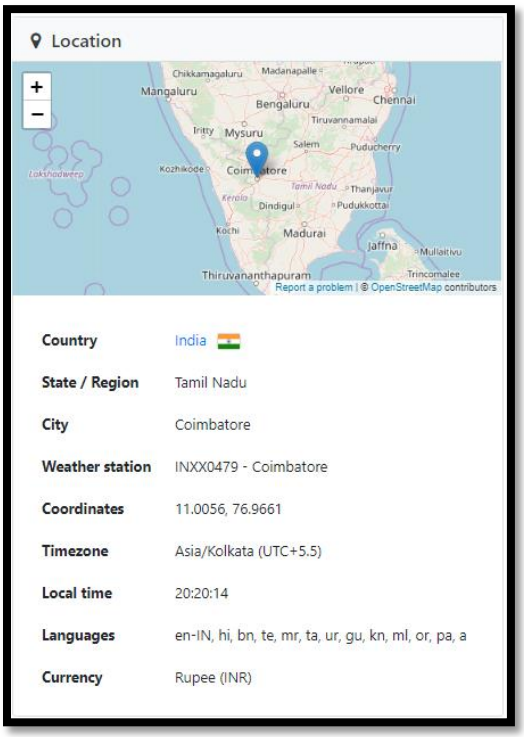
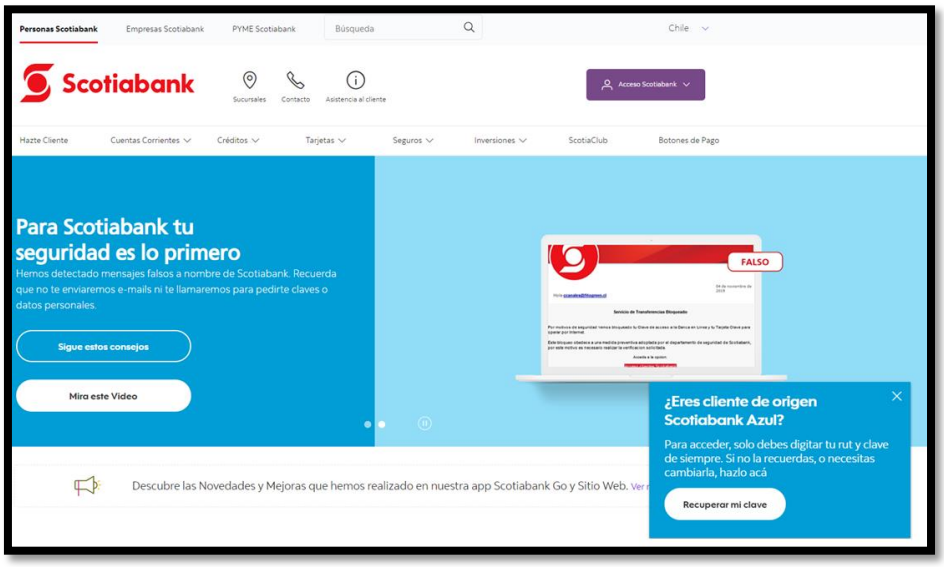
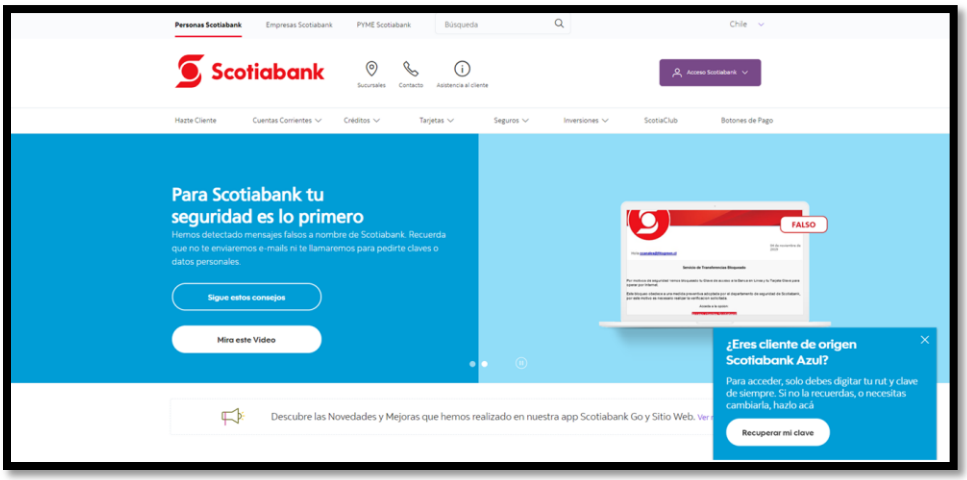
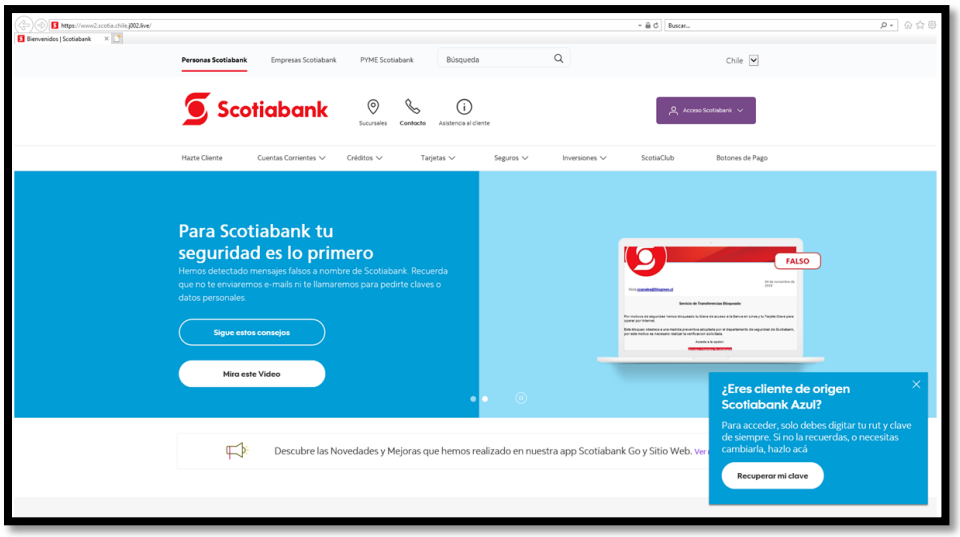


Imagen del sitio

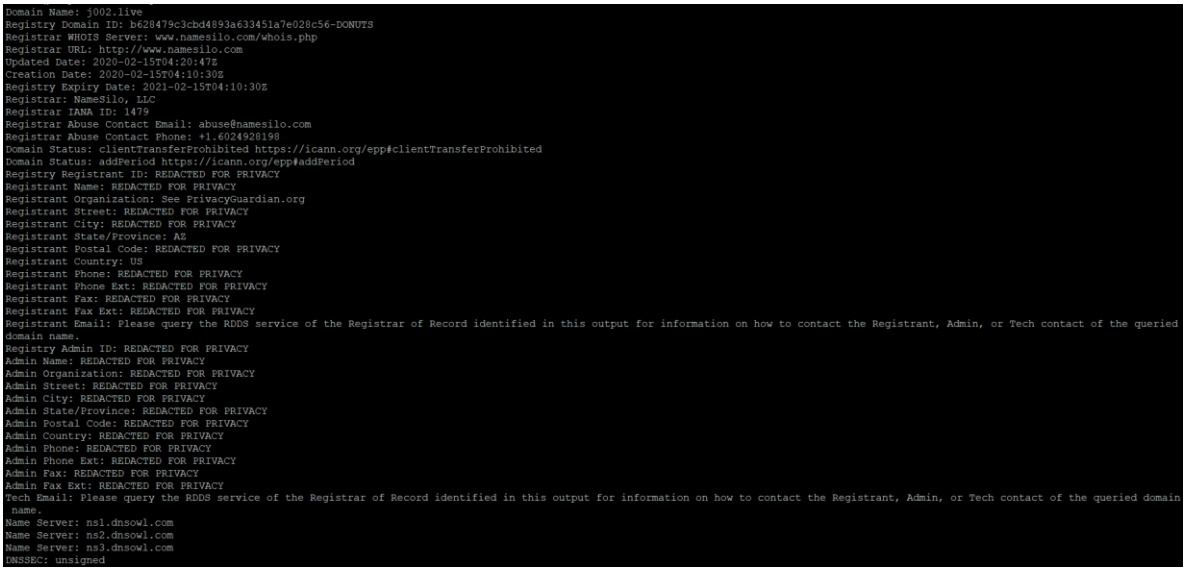



Personas Scotiabank
Empresas Scotiabank
PYME Scotiabank
Búsqueda
Chile
Scotiabank
Sucursales
Contacto
Asistencia al cliente
Acceso Scotiabank
Hazte Cliente
Cuentas Corrientes
Créditos
Tarjetas
Seguros
Inversiones
ScotiaClub
Botones de Pago
Para Scotiabank tu seguridad es lo primero
Hemos detectado mensajes falsos a nombre de Scotiabank. Recuerda que no te enviaremos e-mails ni te llamaremos para pedirte claves o datos personales.
Sigue estos consejos
Mira este Video
FALSO
¿Eres cliente de origen Scotiabank Azul?
Para acceder, solo debes digitar tu rut y clave de siempre. Si no la recuerdas, o necesitas cambiarla, hazlo acá
Recuperar mi clave
Descubre las Novedades y Mejoras que hemos realizado en nuestra app Scotiabank Go y Sitio Web.


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
Para Scotiabank tu seguridad es lo primero
Hemos detectado mensajes falsos a nombre de Scotiabank. Recuerda que no te enviaremos e-mails ni te llamaremos para pedirte claves o datos personales.
Sigue estos consejos
Mira este Video
FALSO
¿Eres cliente de origen Scotiabank Azul?
Para acceder, solo debes digitar tu rut y clave de siempre. Si no la recuerdas, o necesitas cambiarla, hazlo acá
Recuperar mi clave
Descubre las Novedades y Mejoras que hemos realizado en nuestra app Scotiabank Go y Sitio Web.

Whois

```
Domain Name: j002.live
Registry Domain ID: b628479c3cbd4893a63345la7e028c56-DONUTS
Registrar WHOIS Server: www.namesilo.com/whois.php
Registrar URL: http://www.namesilo.com
Updated Date: 2020-02-15T04:20:47Z
Creation Date: 2020-02-15T04:10:30Z
Registry Expiry Date: 2021-02-15T04:10:30Z
Registrar: NameSilo, LLC
Registrar IANA ID: 1479
Registrar Abuse Contact Email: abuse@namesilo.com
Registrar Abuse Contact Phone: +1.6024928198
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: addPeriod https://icann.org/epp#addPeriod
Registry Registrant ID: REDACTED FOR PRIVACY
Registrant Name: REDACTED FOR PRIVACY
Registrant Organization: See PrivacyGuardian.org
Registrant Street: REDACTED FOR PRIVACY
Registrant City: REDACTED FOR PRIVACY
Registrant State/Province: AZ
Registrant Postal Code: REDACTED FOR PRIVACY
Registrant Country: US
Registrant Phone: REDACTED FOR PRIVACY
Registrant Phone Ext: REDACTED FOR PRIVACY
Registrant Fax: REDACTED FOR PRIVACY
Registrant Fax Ext: REDACTED FOR PRIVACY
Registrant Email: Please query the RDDS service of the Registrar of Record identified in this output for infor
mation on how to contact the Registrant, Admin, or Tech contact of the queried domain name.
Registry Admin ID: REDACTED FOR PRIVACY
Admin Name: REDACTED FOR PRIVACY
Admin Organization: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
Admin City: REDACTED FOR PRIVACY
Admin State/Province: REDACTED FOR PRIVACY
Admin Postal Code: REDACTED FOR PRIVACY
Admin Country: REDACTED FOR PRIVACY
Admin Phone: REDACTED FOR PRIVACY
Admin Phone Ext: REDACTED FOR PRIVACY
Admin Fax: REDACTED FOR PRIVACY
Admin Fax Ext: REDACTED FOR PRIVACY
Admin Email: Please query the RDDS service of the Registrar of Record identified in this output for informatio
n on how to contact the Registrant, Admin, or Tech contact of the queried domain name.
Registry Tech ID: REDACTED FOR PRIVACY
Tech Name: REDACTED FOR PRIVACY
Tech Organization: REDACTED FOR PRIVACY
Tech Street: REDACTED FOR PRIVACY
Tech City: REDACTED FOR PRIVACY
Tech State/Province: REDACTED FOR PRIVACY
Tech Postal Code: REDACTED FOR PRIVACY
Tech Country: REDACTED FOR PRIVACY
Tech Phone: REDACTED FOR PRIVACY
Tech Phone Ext: REDACTED FOR PRIVACY
Tech Fax: REDACTED FOR PRIVACY
Tech Fax Ext: REDACTED FOR PRIVACY
Tech Email: Please query the RDDS service of the Registrar of Record identified in this output for information
 on how to contact the Registrant, Admin, or Tech contact of the queried domain name.
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: 2020.02.18 12:36:43 -03'00'