Alerta de seguridad informática	8FFR20-0216-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 de Febrero de 2020
Última revisión	13 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

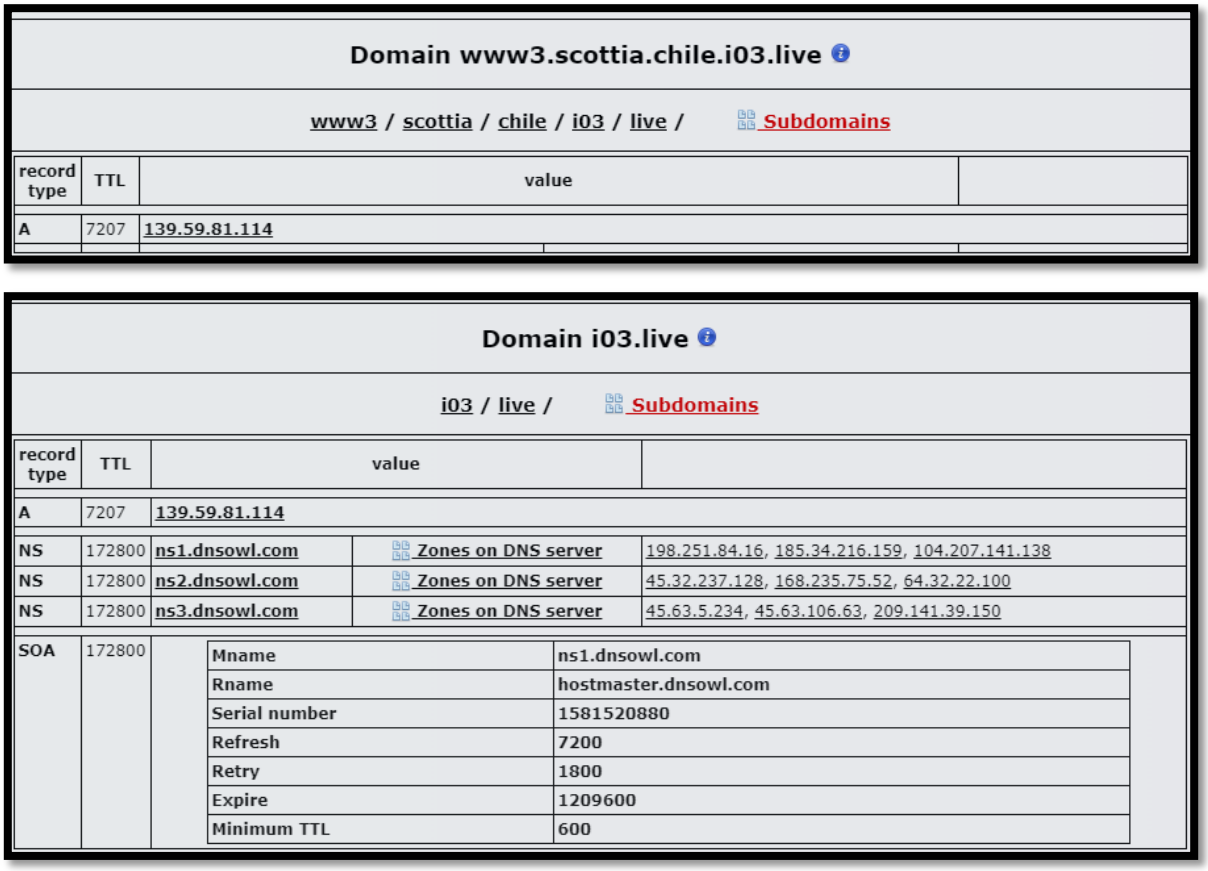
El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de siete portales fraudulentos asociados a una IP que suplanta el sitio web oficial de Banco Scotiabank, el que podría servir para robar credenciales de usuarios de esa entidad.

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
www3[.]scottia[.]chile[.]i03[.]live
www3[.]scottia[.]chile[.]i03[.]live/Personas/
www3[.]scottia[.]chile[.]i03[.]live/login/personas/
www3[.]scottia[.]chile[.]i03[.]live/portalempresas/

Redireccionador de URL´s
dev[.]tdmu[.]edu[.]ua/scotiabank[.]php
forvision[.]ru/scotiabank[.]php
www[.]gacaaward[.]org/scotiabank[.]php



Domain www3.scottia.chile.i03.live

www3 / scottia / chile / i03 / live / Subdomains

record type	TTL	value
A	7207	139.59.81.114

Domain i03.live

i03 / live / Subdomains

record type	TTL	value		
A	7207	139.59.81.114		
NS	172800	ns1.dnsowl.com	Zones on DNS server	198.251.84.16, 185.34.216.159, 104.207.141.138
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	45.63.5.234, 45.63.106.63, 209.141.39.150

SOA	172800	Mname	ns1.dnsowl.com
		Rname	hostmaster.dnsowl.com
		Serial number	1581520880
		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=www3.scottia.chile.i03.live
Issuer DN	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
Serial	397573414752828197257265708010655830423908
Validity	2020-02-11 19:44:25 **to** 2020-05-11 19:44:25 (90 days, 0:00:00)
Names	www3.scottia.chile.i03.live

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

IP
139[.]59[.]81[.]114

Domain www3.scottia.chile.i03.live is located on IP address << 139.59.81.114 >>

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
Country	SG , Singapore
Host name	no record in reverse zone

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

Localización
Bangalore, Karnataka, India

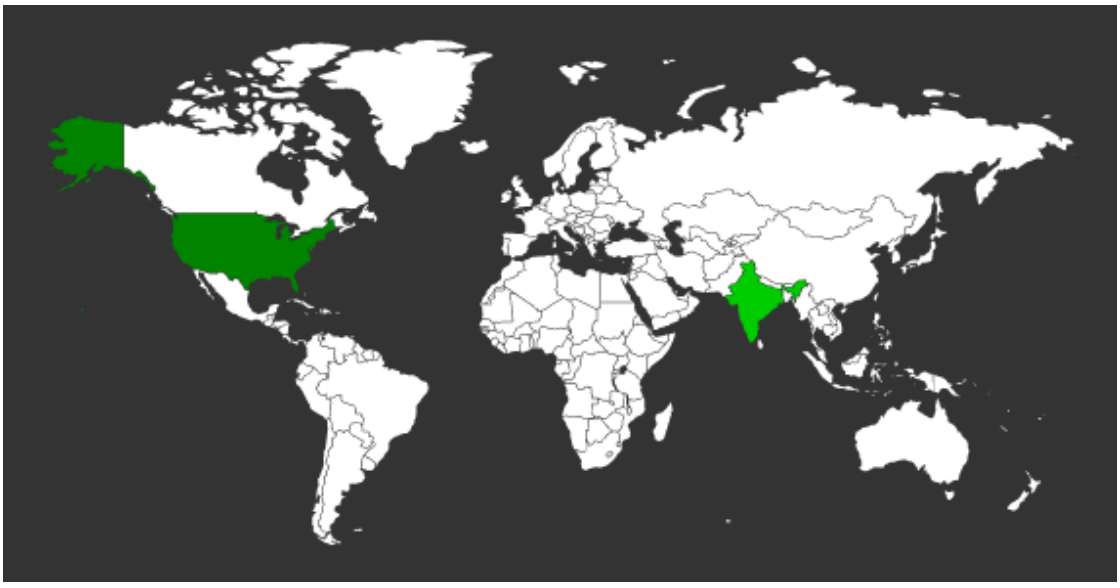
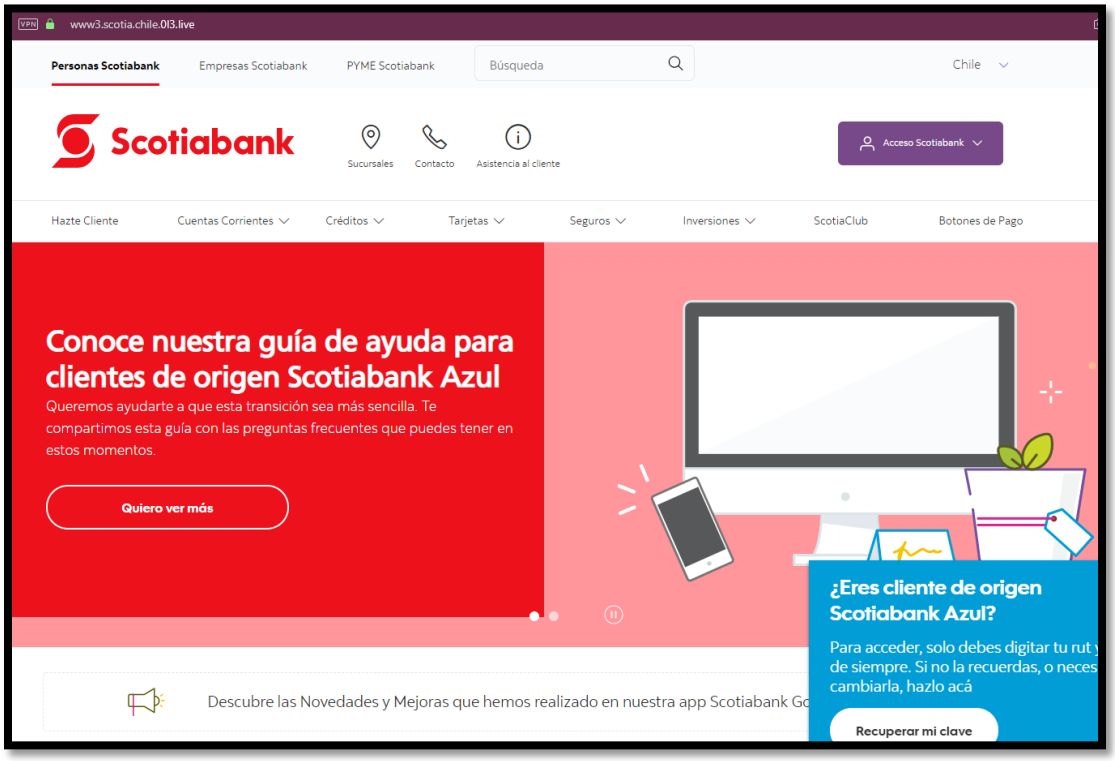


Imagen del sitio



Whois

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

refer:        whois.nic.live

domain:       LIVE

organisation: United TLD Holdco Ltd.
address:      One Clarendon Row, Dublin 2, Co. Dublin
address:      Ireland

contact:      administrative
name:         Serina Ness
organisation: Donuts Inc.
address:      Donuts Inc.
address:      5808 Lake Washington Blvd NE, Suite 300
address:      Kirkland, WA 98033
address:      United States
phone:        +1.425.283.8248
fax-no:       +1.425.671.0020
e-mail:       serina@donuts.email

contact:      technical
name:         Ben Levac
organisation: Donuts Inc.
address:      Donuts Inc.
address:      5808 Lake Washington Blvd NE, Suite 300
address:      Kirkland, WA 98033
address:      United States
phone:        +1.425.298.2200
fax-no:       +1.425.671.0020
e-mail:       ben@donuts.email

nserver:      DEMAND.ALPHA.ARIDNS.NET.AU 2001:dcd:1:0:0:0:0:7 37.209.192.7
nserver:      DEMAND.BETA.ARIDNS.NET.AU 2001:dcd:2:0:0:0:0:7 37.209.194.7
nserver:      DEMAND.DELTA.ARIDNS.NET.AU 2001:dcd:4:0:0:0:0:7 37.209.198.7
nserver:      DEMAND.GAMMA.ARIDNS.NET.AU 2001:dcd:3:0:0:0:0:7 37.209.196.7
ds-rdata:     30640 8 1 B1B3A0ED44A1DEA6B8AC937937426B0887C6C4AC
ds-rdata:     30640 8 2 C2A186F6BD89AE983EE147EDCE3148A75343EE1F12869ABBCF293388457F495D

whois:        whois.nic.live

status:       ACTIVE
remarks:      Registration information: http://www.donuts.domains/

created:      2015-06-25
changed:      2019-08-01
source:       IANA

Domain Name: i03.live
Registry Domain ID: d6289c02cfa04e24b0c971a7aef970c1-DONUTS
Registrar WHOIS Server: www.namesilo.com/whois.php
Registrar URL: http://www.namesilo.com
Updated Date: 2020-02-11T19:47:37Z
Creation Date: 2020-02-11T19:44:00Z
Registry Expiry Date: 2021-02-11T19:44:00Z
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
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of WHOIS database: 2020-02-12T15:54:53Z <<<

For more information on Whois status codes, please visit https://icann.org/epp

Terms of Use: Donuts Inc. provides this Whois service for information purposes, and to assist persons in obtai
ning information about or related to a domain name registration record. Donuts does not guarantee its accuracy
. Users accessing the Donuts Whois service agree to use the data only for lawful purposes, and under no circum
stances may this data be used to: a) allow, enable, or otherwise support the transmission by e-mail, telephone
, or facsimile of mass unsolicited, commercial advertising or solicitations to entities other than the registr
ar's own existing customers and b) enable high volume, automated, electronic processes that send queries or da
ta to the systems of Donuts or any ICANN-accredited registrar, except as reasonably necessary to register doma
in names or modify existing registrations. When using the Donuts Whois service, please consider the following:
The Whois service is not a replacement for standard EPP commands to the SRS service. Whois is not considered
authoritative for registered domain objects. The Whois service may be scheduled for downtime during production
or OT&E maintenance periods. Queries to the Whois services are throttled. If too many queries are received fr
om a single IP address within a specified time, the service will begin to reject further queries for a period
```

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: 2020.02.13 15:38:58 -03'00'