Alerta de seguridad informática	8FFR20-00286-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	26 de Marzo de 2020
Última revisión	26 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 un portal fraudulento asociado a una IP que suplanta el sitio web oficial de 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 COMPROMISO

URL
scotia[.]chileacessomovil[.]com
scotia[.]chileacessomovil[.]com/site/web/acesso[.]php
IP
80[.]211[.]130[.]144

DOMINIOS DONDE SE ALOJA URL

Domain scotia.chileacessomovil.com

scotia / chileacessomovil / com / Subdomains

record type	TTL	value
A	3600	80.211.130.144

Domain chileacessomovil.com

chileacessomovil / com / Subdomains

record type	TTL	value		
NS	21600	ns-cloud-a1.googledomains.com	Zones on DNS server	216.239.32.106
NS	21600	ns-cloud-a2.googledomains.com	Zones on DNS server	216.239.34.106
NS	21600	ns-cloud-a3.googledomains.com	Zones on DNS server	216.239.36.106
NS	21600	ns-cloud-a4.googledomains.com	Zones on DNS server	216.239.38.106

SOA	21600		
		Mname	ns-cloud-a1.googledomains.com
		Rname	cloud-dns-hostmaster.google.com
		Serial number	6
		Refresh	21600
		Retry	3600
		Expire	259200
		Minimum TTL	300

CERTIFICADOS

Subject DN	CN=scotia.chileacessomovil.com
Issuer DN	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
Serial	304028855158609878912352567588110812408982
Validity	2020-03-18 21:13:53 **to** 2020-06-16 21:13:53 (90 days, 0:00:00)
Names	scotia.chileacessomovil.com

IP DE ORIGEN DONDE SE ALOJA SITIO

Domain scotia.chileacessomovil.com is located on IP address << 80.211.130.144 >>

Block start	80.211.130.0
End of block	80.211.130.255
Block size	256 Domains in block
Block name	ARUBA-NET
AS number	31034
Parent block	80.211.128.0 - 80.211.191.255
Organization	Aruba S.p.A. - Cloud Services Farm2

LOCALIZACIÓN

Arezzo, Toscana, Italia

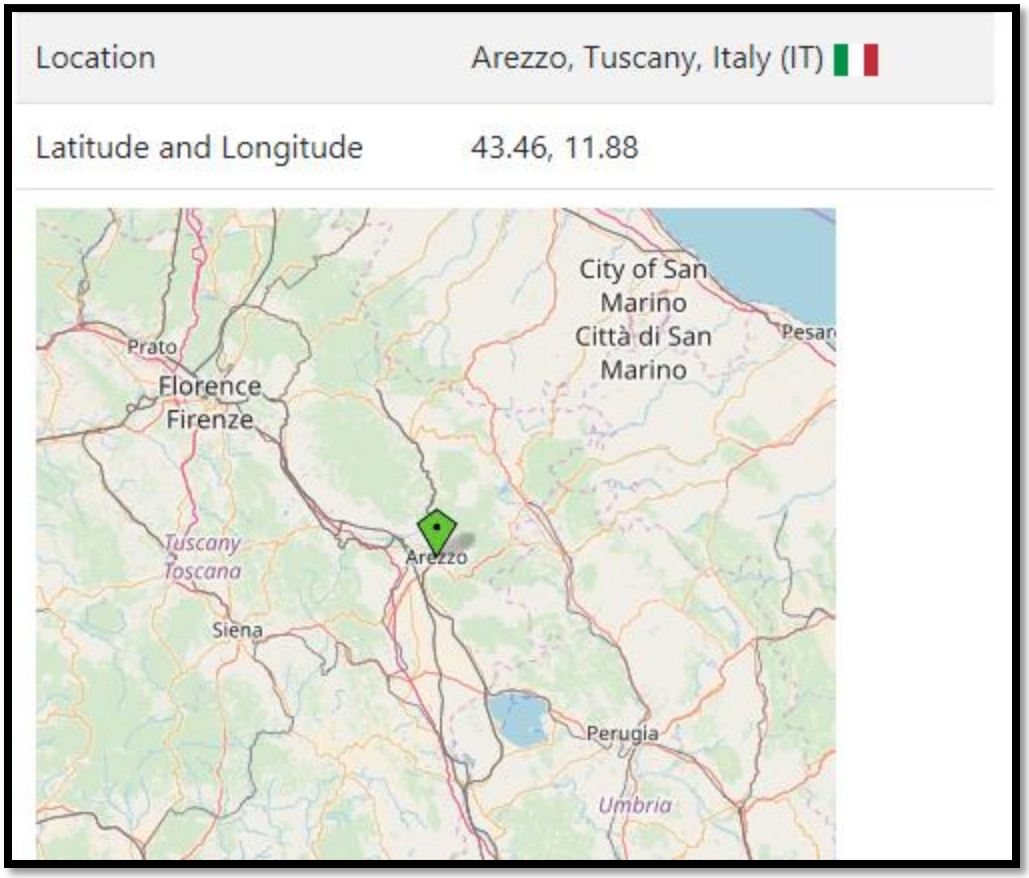
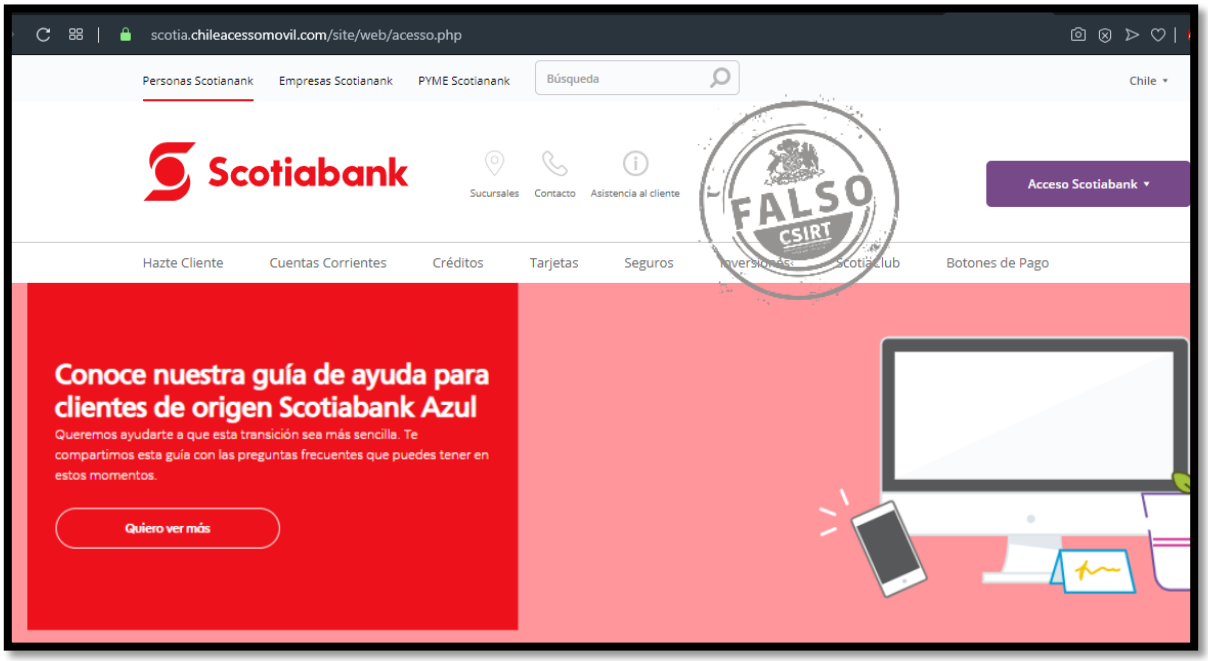


IMAGEN DEL SITIO



WHOIS

```
Domain Name: chileacessomovil.com
Registry Domain ID: 2504845931_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.google.com
Registrar URL: https://domains.google.com
Updated Date: 2020-03-18T18:39:08Z
Creation Date: 2020-03-18T18:39:07Z
Registrar Registration Expiration Date: 2021-03-18T18:39:07Z
Registrar: Google LLC
Registrar IANA ID: 895
Registrar Abuse Contact Email: registrar-abuse@google.com
Registrar Abuse Contact Phone: +1.8772376466
Domain Status: clientTransferProhibited https://www.icann.org/epp#clientTransferProhibited
Registry Registrant ID:
Registrant Name: Contact Privacy Inc. Customer 1246707704
Registrant Organization: Contact Privacy Inc. Customer 1246707704
Registrant Street: 96 Mowat Ave
Registrant City: Toronto
Registrant State/Province: ON
Registrant Postal Code: M4K 3K1
Registrant Country: CA
Registrant Phone: +1.4165385487
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: m4egn7wnjvnr@contactprivacy.email
Registry Admin ID:
Admin Name: Contact Privacy Inc. Customer 1246707704
Admin Organization: Contact Privacy Inc. Customer 1246707704
Admin Street: 96 Mowat Ave
Admin City: Toronto
Admin State/Province: ON
Admin Postal Code: M4K 3K1
Admin Country: CA
Admin Phone: +1.4165385487
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: m4egn7wnjvnr@contactprivacy.email
Registry Tech ID:
Tech Name: Contact Privacy Inc. Customer 1246707704
Tech Organization: Contact Privacy Inc. Customer 1246707704
Tech Street: 96 Mowat Ave
Tech City: Toronto
Tech State/Province: ON
Tech Postal Code: M4K 3K1
Tech Country: CA
Tech Phone: +1.4165385487
Tech Phone Ext:
Tech Fax:
```

```
Tech Fax Ext:
Tech Email: m4egn7wnjvnr@contactprivacy.email
Name Server: NS-CLOUD-A1.GOOGLEDOMAINS.COM
Name Server: NS-CLOUD-A2.GOOGLEDOMAINS.COM
Name Server: NS-CLOUD-A3.GOOGLEDOMAINS.COM
Name Server: NS-CLOUD-A4.GOOGLEDOMAINS.COM
DNSSEC: signedDelegation
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2020-03-25T19:44:22Z <<<
```

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: 2020.03.26 09:51:50 -03'00'