Alerta de seguridad informática	**8FFR-00077-001**
Clase de alerta	**Fraude**
Tipo de incidente	**Falsificación de Registros o Identidad**
Nivel de riesgo	**Alto**
TLP	**Blanco**
Fecha de lanzamiento original	**03 de Octubre de 2019**
Última revisión	**03 de Octubre de 2019**

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 **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

https[://]www[.]scotiabankchile[.]net/choose[.]php

Domain scotiabankchile.net

scotiabankchile / net / Subdomains

record type	TTL	value		
A	3600	162.241.203.25		
NS	21600	ns-cloud-c1.googledomains.com	Zones on DNS server	216.239.32.108
NS	21600	ns-cloud-c2.googledomains.com	Zones on DNS server	216.239.34.108
NS	21600	ns-cloud-c3.googledomains.com	Zones on DNS server	216.239.36.108
NS	21600	ns-cloud-c4.googledomains.com	Zones on DNS server	216.239.38.108
SOA	21600	Mname: ns-cloud-c1.googledomains.com Rname: cloud-dns-hostmaster.google.com Serial number: 4 Refresh: 21600 Retry: 3600 Expire: 259200 Minimum TTL: 300		

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

Certificado

Criteria	Identity = 'scotiabankchile.net'

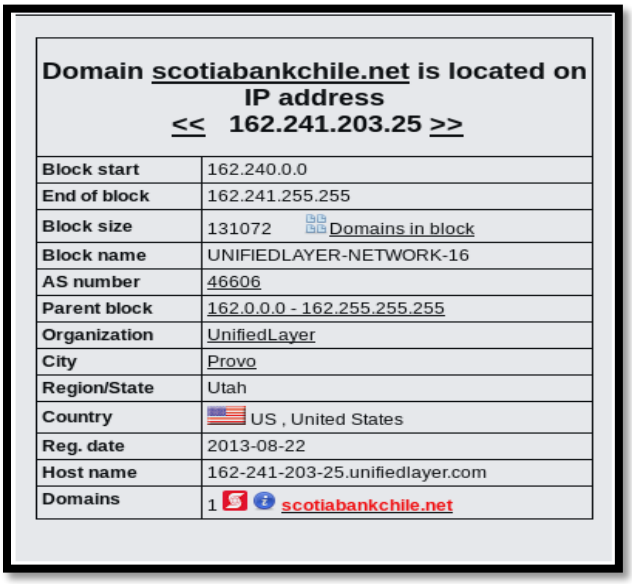
Certificates

crt.sh ID	Logged At ⇧	Not Before	Not After	Issuer Name
1949630385	2019-10-02	2019-10-02	2019-12-31	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´s

162[.]241[.]203[.]25



Domain scotiabankchile.net is located on IP address
<< 162.241.203.25 >>

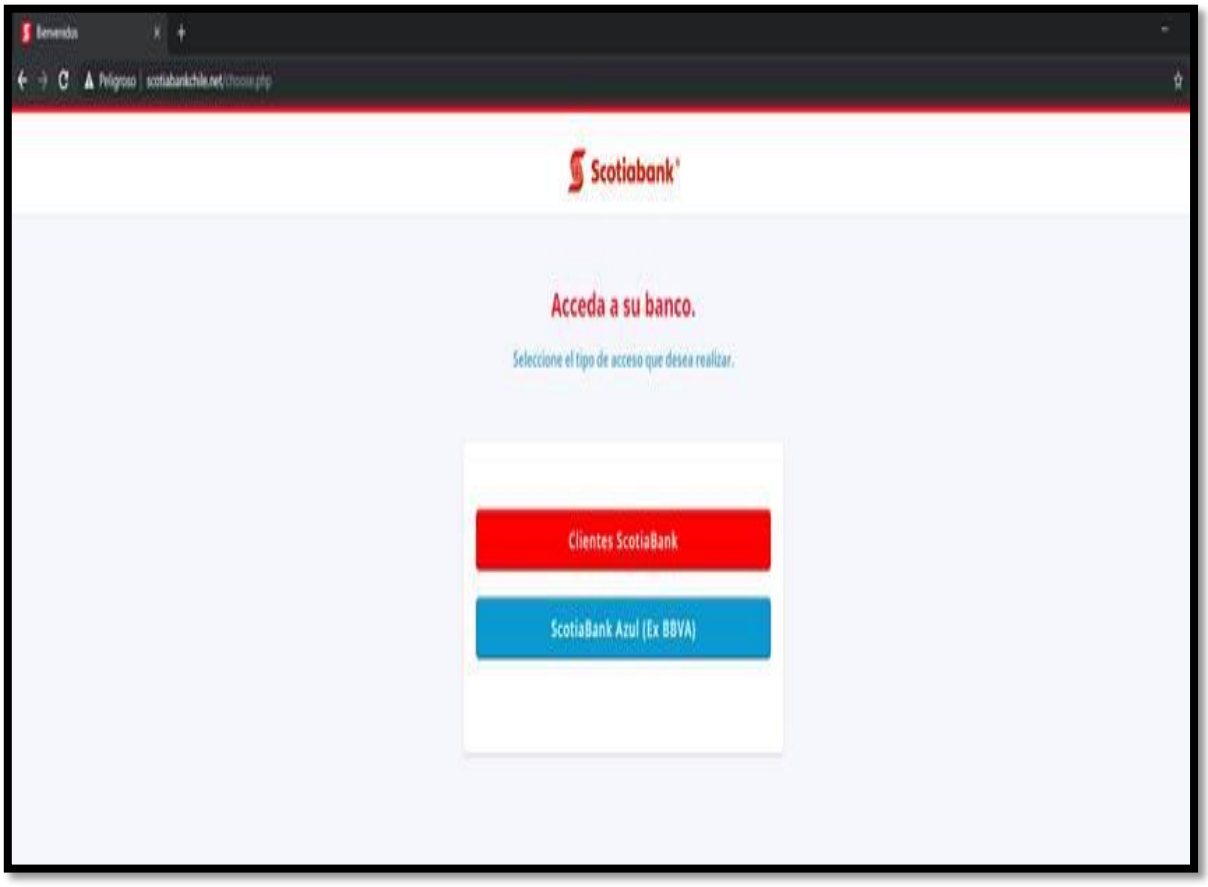
Block start	162.240.0.0
End of block	162.241.255.255
Block size	131072 Domains in block
Block name	UNIFIEDLAYER-NETWORK-16
AS number	46606
Parent block	162.0.0.0 - 162.255.255.255
Organization	UnifiedLayer
City	Provo
Region/State	Utah
Country	US , United States
Reg. date	2013-08-22
Host name	162-241-203-25.unifiedlayer.com
Domains	1 scotiabankchile.net

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

Localización

Provo, Utah, Estados Unidos

Imagen del sitio



Whois

```
soc@misp:~$ whois -h whois.google.com scotiabankchile.net
Domain Name: scotiabankchile.net
Registry Domain ID: 2439492774_DOMAIN_NET-VRSN
Registrar WHOIS Server: whois.google.com
Registrar URL: https://domains.google.com
Updated Date: 2019-10-02T15:19:59Z
Creation Date: 2019-10-02T15:19:58Z
Registrar Registration Expiration Date: 2020-10-02T15:19:58Z
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 1245580147
Registrant Organization: Contact Privacy Inc. Customer 1245580147
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: sebtpuj8ixqf@contactprivacy.email
Registry Admin ID:
Admin Name: Contact Privacy Inc. Customer 1245580147
Admin Organization: Contact Privacy Inc. Customer 1245580147
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: sebtpuj8ixqf@contactprivacy.email
Registry Tech ID:
Tech Name: Contact Privacy Inc. Customer 1245580147
Tech Organization: Contact Privacy Inc. Customer 1245580147
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: sebtpuj8ixqf@contactprivacy.email
Name Server: NS-CLOUD-C1.GOOGLEDOMAINS.COM
Name Server: NS-CLOUD-C2.GOOGLEDOMAINS.COM
Name Server: NS-CLOUD-C3.GOOGLEDOMAINS.COM
Name Server: NS-CLOUD-C4.GOOGLEDOMAINS.COM
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2019-10-03T11:37:01Z <<<

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

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: 2019.10.03 13:08:14 -03'00'