Alerta de seguridad informática	**8FFR-00089-001**
Clase de alerta	**Fraude**
Tipo de incidente	**Falsificación de Registros o Identidad**
Nivel de riesgo	**Alto**
TLP	**Blanco**
Fecha de lanzamiento original	**14 de Octubre de 2019**
Última revisión	**14 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 redirige a sitios que suplantan el sitio web oficial de **Banco Scotiabank**, lo 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[.]scotiabankchilemobile[.]com/choose[.]php

Domain scotiabankchilemobile.com

scotiabankchilemobile / com / Subdomains

record type	TTL	value		
A	3600	162.241.203.26		
NS	21600	ns-cloud-e1.googledomains.com	Zones on DNS server	216.239.32.110
NS	21600	ns-cloud-e2.googledomains.com	Zones on DNS server	216.239.34.110
NS	21600	ns-cloud-e3.googledomains.com	Zones on DNS server	216.239.36.110
NS	21600	ns-cloud-e4.googledomains.com	Zones on DNS server	216.239.38.110
SOA	21600	Mname: ns-cloud-e1.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

IP´s

162[.]241[.]203[.]26

Domain scotiabankchilemobile.com is located on IP address << 162.241.203.26 >>

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	162-241-203-26.unifiedlayer.com
Domain count	>= 2 Servers around
Domains	1 scotiabankchilemobile.com 2 scotiabankcl.org

Ilustración 2 Ip de Origen donde se aloja Sitio Falso del Banco Scotiabank

Localización

Provo, Utah, Estados Unidos

Certificados

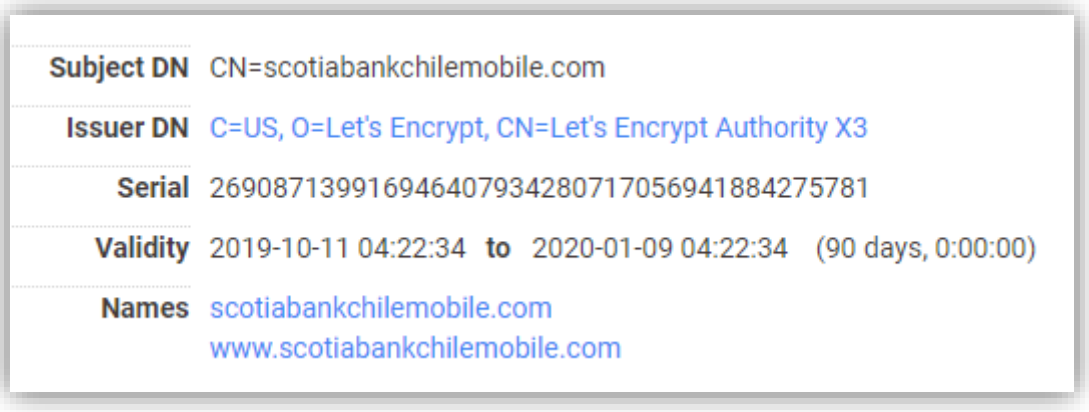
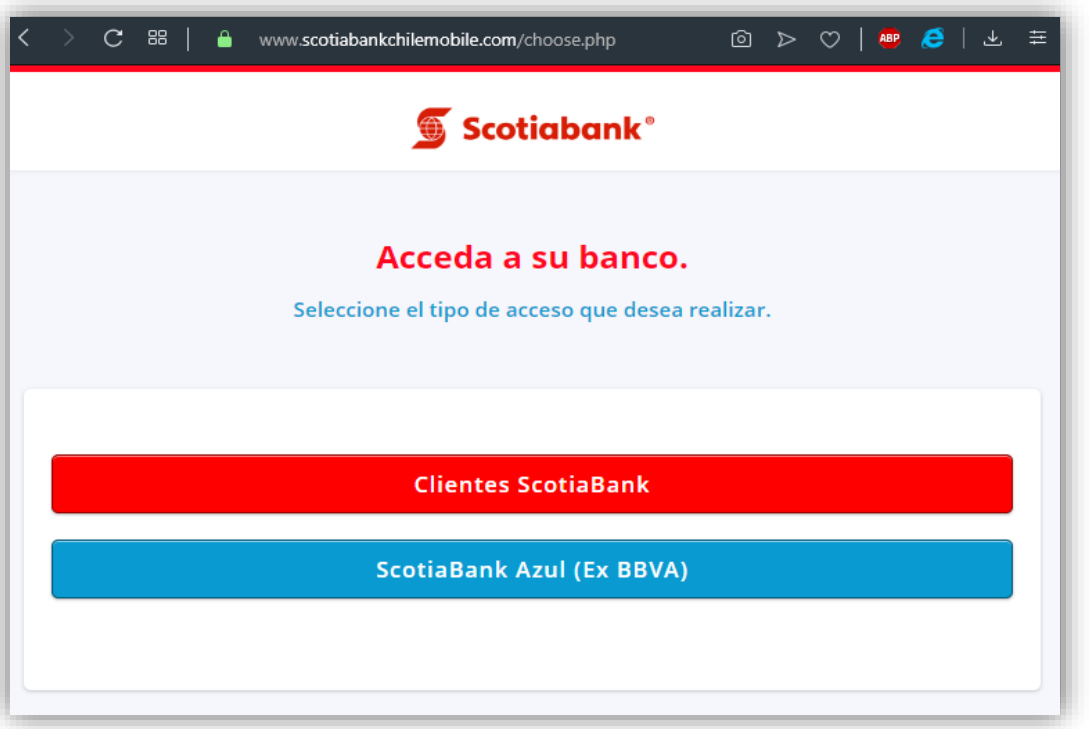


Ilustración 3 Certificado Utilizado en Url del sitio Falso del Banco Scotiabank

Imagen del sitio



Whois

```
Domain Name: N4NTUCKET.BEST
Registry Domain ID: D134208070-CNIC
Registrar WHOIS Server: whois.dynadot.com
Registrar URL: http://www.dynadot.com
Updated Date: 2019-10-10T15:45:49.0Z
Creation Date: 2019-10-10T05:22:36.0Z
Registry Expiry Date: 2020-10-10T23:59:59.0Z
Registrar: Dynadot LLC
Registrar IANA ID: 472
Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: addPeriod https://icann.org/epp#addPeriod
Registrant Organization:
Registrant State/Province: California
Registrant Country: US
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.
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.
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: DALNS5.MASTERNS.COM
Name Server: DALNS6.MASTERNS.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: 2019.10.14 20:45:05 -03'00'