Alerta de seguridad informática	8FFR-00135-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	1 de Diciembre de 2019
Última revisión	1 de Diciembre 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

URL Sitio Clonado:
https[://]scotia[.]bankgo[.]org/site/choose-type[.]php

Domain scotia.bankgo.org

scotia / bankgo / org / Subdomains

record type	TTL	value	
A	3600	162.241.203.25	

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

Certificados

Criteria	Identity = 'scotia.bankgo.org'

Certificates

crt.sh ID	Logged At ⇧	Not Before	Not After	Issuer Name
2052235032	2019-10-30	2019-10-29	2020-01-27	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
2049975106	2019-10-30	2019-10-29	2020-01-27	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

162.241.203.25

Domain scotia.bankgo.org 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

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

Localización

Provo, Utah, Estados Unidos

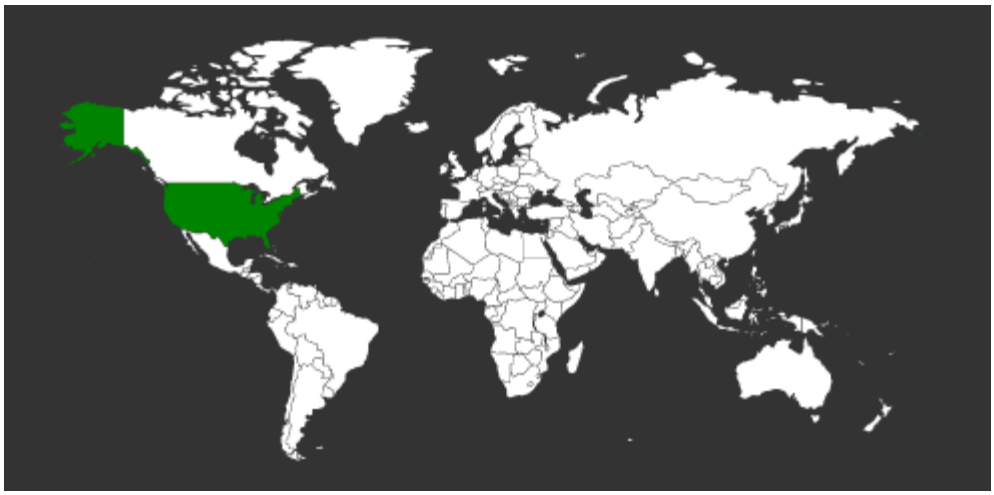
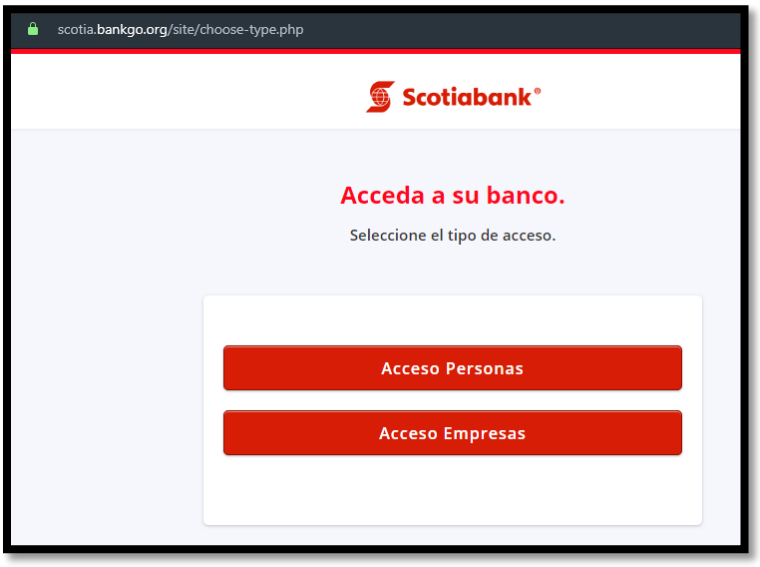
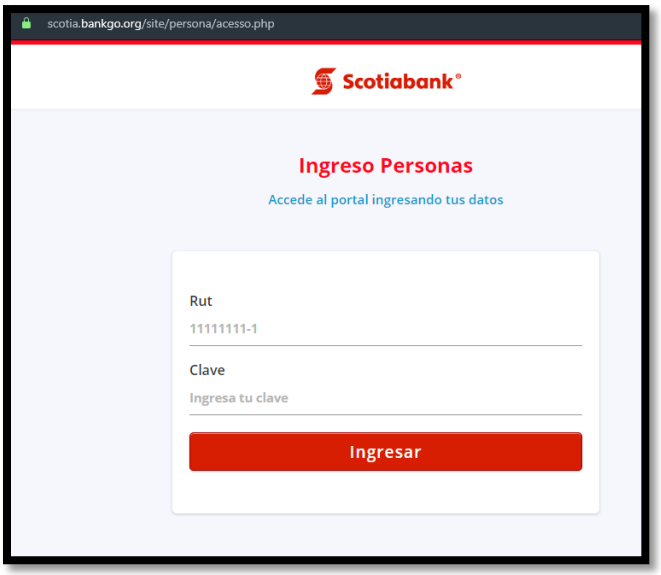
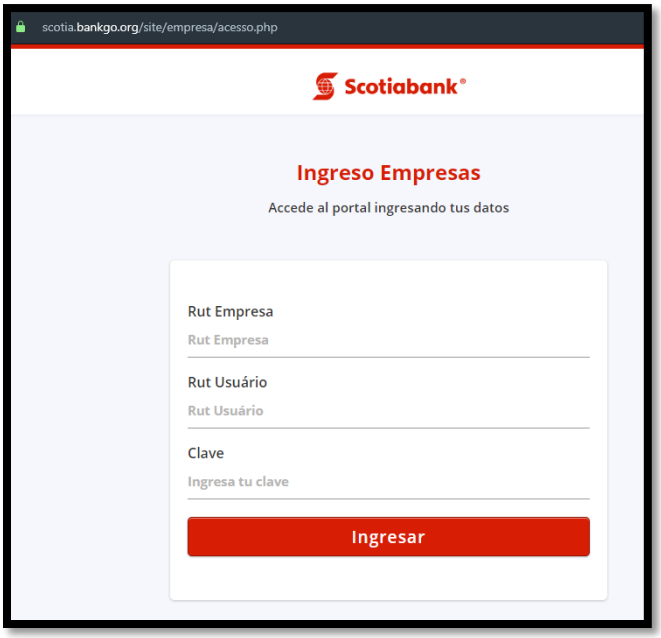


Imagen del sitio




scotia.bankgo.org/site/persona/acesso.php
Scotiabank
Ingreso Personas
Accede al portal ingresando tus datos
Rut
11111111-1
Clave
Ingresa tu clave
Ingresar


scotia.bankgo.org/site/empresa/acesso.php
Scotiabank
Ingreso Empresas
Accede al portal ingresando tus datos
Rut Empresa
Rut Empresa
Rut Usuário
Rut Usuário
Clave
Ingresa tu clave
Ingresar

Whois

```
Domain Name: bankgo.org
Registry Domain ID: D402200000011764496-LROR
Registrar WHOIS Server: whois.google.com
Registrar URL: https://domains.google.com
Updated Date: 2019-10-29T19:18:50Z
Creation Date: 2019-10-29T19:18:47Z
Registrar Registration Expiration Date: 2020-10-29T19:18:47Z
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
Domain Status: serverTransferProhibited https://www.icann.org/epp#serverTransferProhibited
Registry Registrant ID: go-14100793600
Registrant Name: Contact Privacy Inc. Customer 1245764899
Registrant Organization: Contact Privacy Inc. Customer 1245764899
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: 7dshqrypomnq@contactprivacy.email
Registry Admin ID: go-14100793600
Admin Name: Contact Privacy Inc. Customer 1245764899
Admin Organization: Contact Privacy Inc. Customer 1245764899
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: 7dshqrypomnq@contactprivacy.email
Registry Tech ID: go-14100793600
Tech Name: Contact Privacy Inc. Customer 1245764899
Tech Organization: Contact Privacy Inc. Customer 1245764899
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: 7dshqrypomnq@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: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2019-11-27T13:50:18Z <<<
```

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.