Alerta de seguridad informática	8FFR20-00194-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	26 de Enero de 2020
Última revisión	26 de Enero 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 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

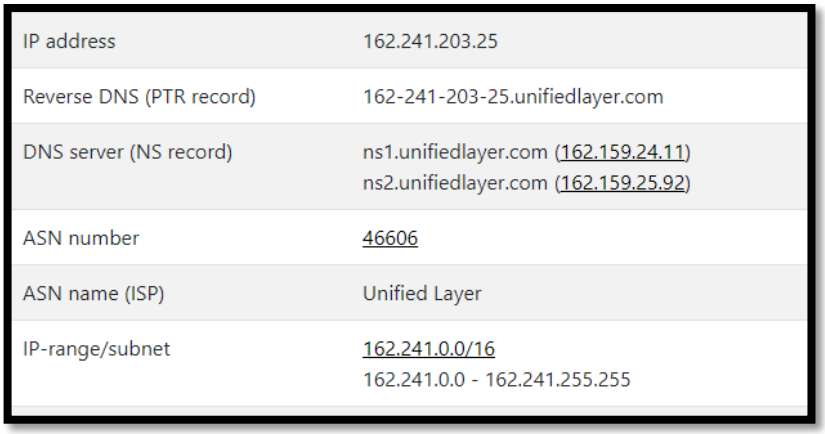
scotia[.]chilemv[.]com/site/web/acesso[.]php

Certificados

Ilustración 1 Certificado Utilizado en Url del sitio Falso del Banco Scotiabank.

IP

162.241.203.25



IP address	162.241.203.25
Reverse DNS (PTR record)	162-241-203-25.unifiedlayer.com
DNS server (NS record)	ns1.unifiedlayer.com (162.159.24.11) ns2.unifiedlayer.com (162.159.25.92)
ASN number	46606
ASN name (ISP)	Unified Layer
IP-range/subnet	162.241.0.0/16 162.241.0.0 - 162.241.255.255

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

Localización

Provo, Utah, Estados Unidos

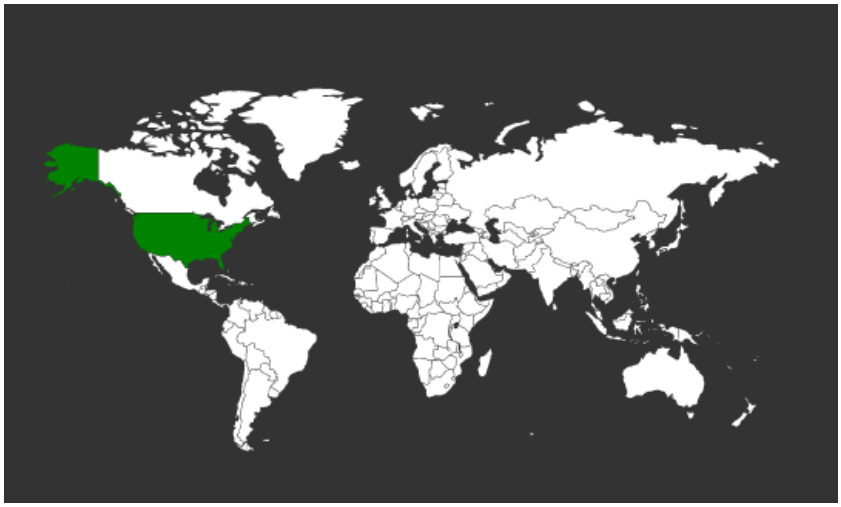
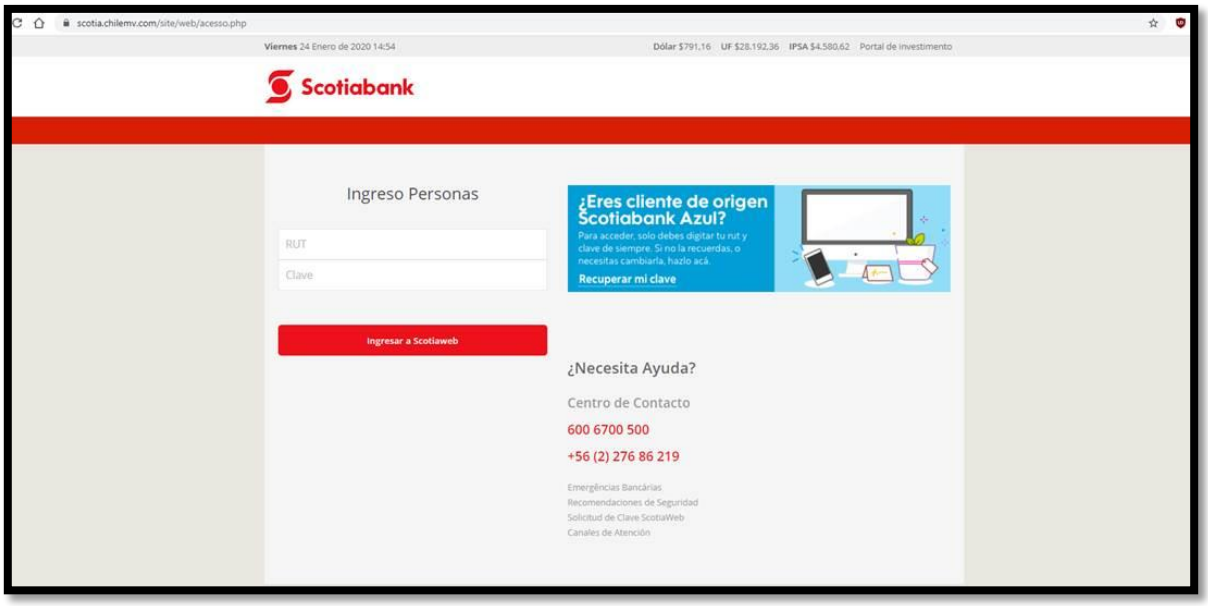
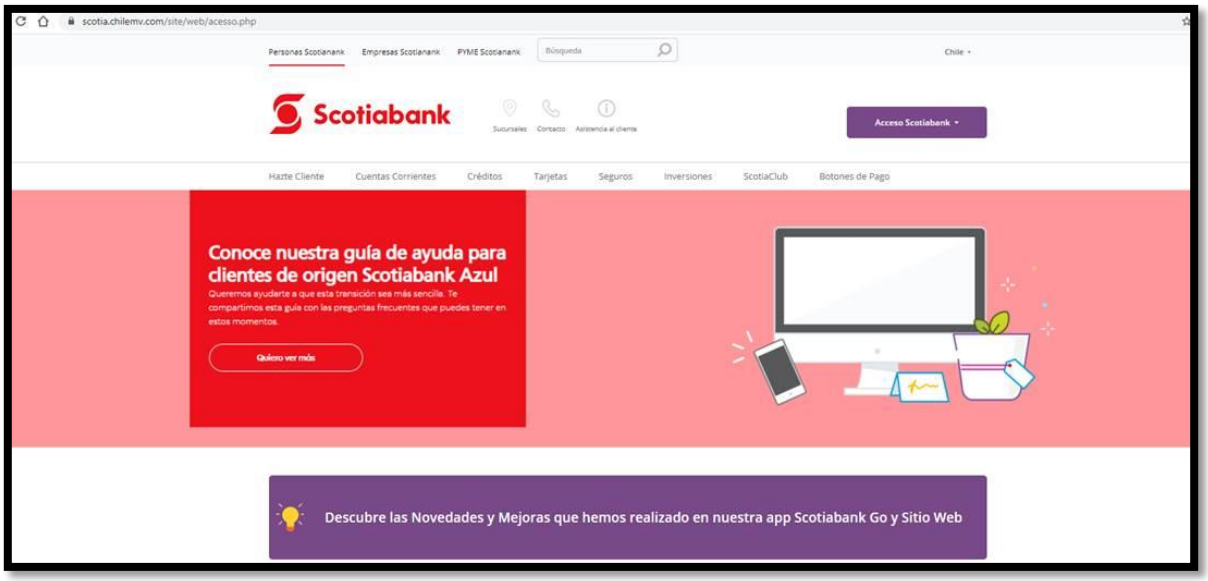


Imagen del sitio





Whois

```
Domain Name: chilemv.com
Registry Domain ID: 2442462680_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.google.com
Registrar URL: https://domains.google.com
Updated Date: 2020-01-24T13:27:16Z
Creation Date: 2019-10-11T07:22:49Z
Registrar Registration Expiration Date: 2020-10-11T07:22:53Z
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: clientDeleteProhibited https://www.icann.org/epp#clientDeleteProhibited
Domain Status: clientUpdateProhibited https://www.icann.org/epp#clientUpdateProhibited
Domain Status: clientHold https://www.icann.org/epp#clientHold
Registry Registrant ID:
Registrant Name: Contact Privacy Inc. Customer 1245638340
Registrant Organization: Contact Privacy Inc. Customer 1245638340
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: z5llhsswm0hk@contactprivacy.email
Registry Admin ID:
Admin Name: Contact Privacy Inc. Customer 1245638340
Admin Organization: Contact Privacy Inc. Customer 1245638340
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: z5llhsswm0hk@contactprivacy.email
Registry Tech ID:
Tech Name: Contact Privacy Inc. Customer 1245638340
Tech Organization: Contact Privacy Inc. Customer 1245638340
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: z5llhsswm0hk@contactprivacy.email
Name Server: ns-cloud-b1.googledomains.com
Name Server: ns-cloud-b2.googledomains.com
Name Server: ns-cloud-b3.googledomains.com
Name Server: ns-cloud-b4.googledomains.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.