Alerta de seguridad informática	8FFR20-00233-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	28 de Febrero de 2020
Última revisión	28 de Febrero 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 del 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

URLs

scotiachile[.]cl-support[.]login[.]themotoringbusiness[.]com/scoticheyo2020

Domain themotoringbusiness.com

themotoringbusiness / com / Subdomains

record type	TTL	value		
A	14400	192.185.37.184		
NS	86400	ns8013.hostgator.com	Zones on DNS server	192.185.5.111
NS	86400	ns8014.hostgator.com	Zones on DNS server	192.185.5.112
MX	14400	0 mail.themotoringbusiness.com		
TXT	14400	v=spf1 a mx include:websitewelcome.com ~all		

SOA	86400	Mname	ns8013.hostgator.com
		Rname	root.gator4007.hostgator.com
		Serial number	2020022703
		Refresh	86400
		Retry	7200
		Expire	3600000
		Minimum TTL	86400

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

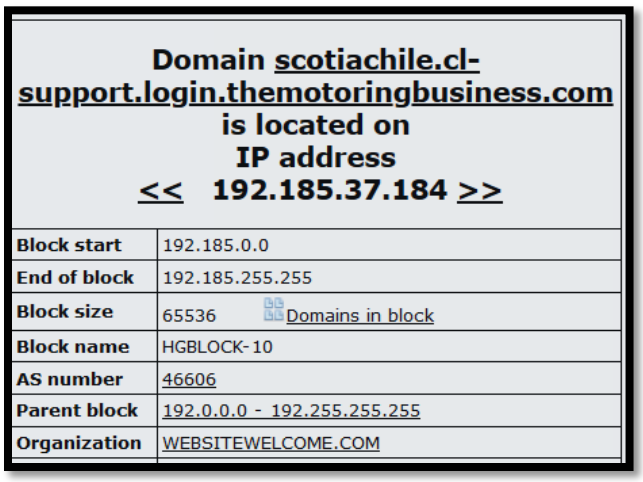
Certificados

Subject DN	CN=scotiachile.cl-support.login.themotoringbusiness.com
Issuer DN	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
Serial	346453546130344235135392989807558427853898
Validity	2020-02-27 06:14:33 **to** 2020-05-27 06:14:33 (90 days, 0:00:00)
Names	scotiachile.cl-support.login.themotoringbusiness.com www.scotiachile.cl-support.login.themotoringbusiness.com

Ilustración 2 Certificado Utilizado en Url del sitio Falso del Banco Scotiabank

IP

192[.]185[.]37[.]184



Domain scotiachile.cl-support.login.themotoringbusiness.com is located on IP address << 192.185.37.184 >>

Block start	192.185.0.0
End of block	192.185.255.255
Block size	65536 Domains in block
Block name	HGBLOCK-10
AS number	46606
Parent block	192.0.0.0 - 192.255.255.255
Organization	WEBSITEWELCOME.COM

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

Localización

Provo, Utah, United States of America

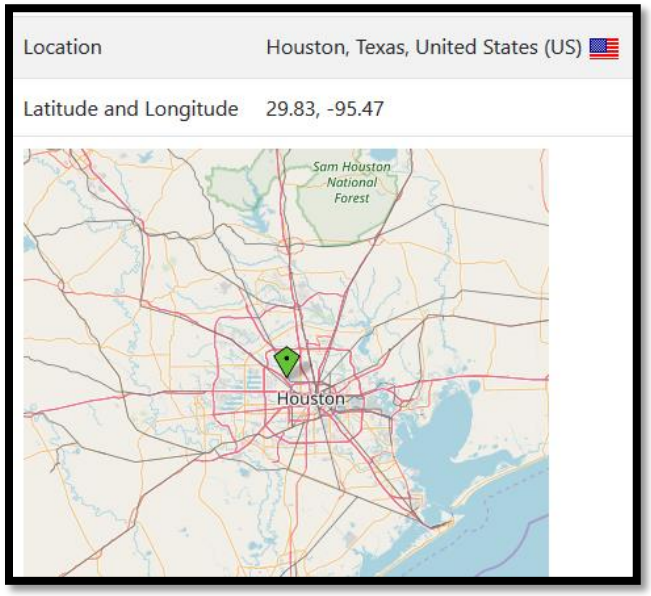
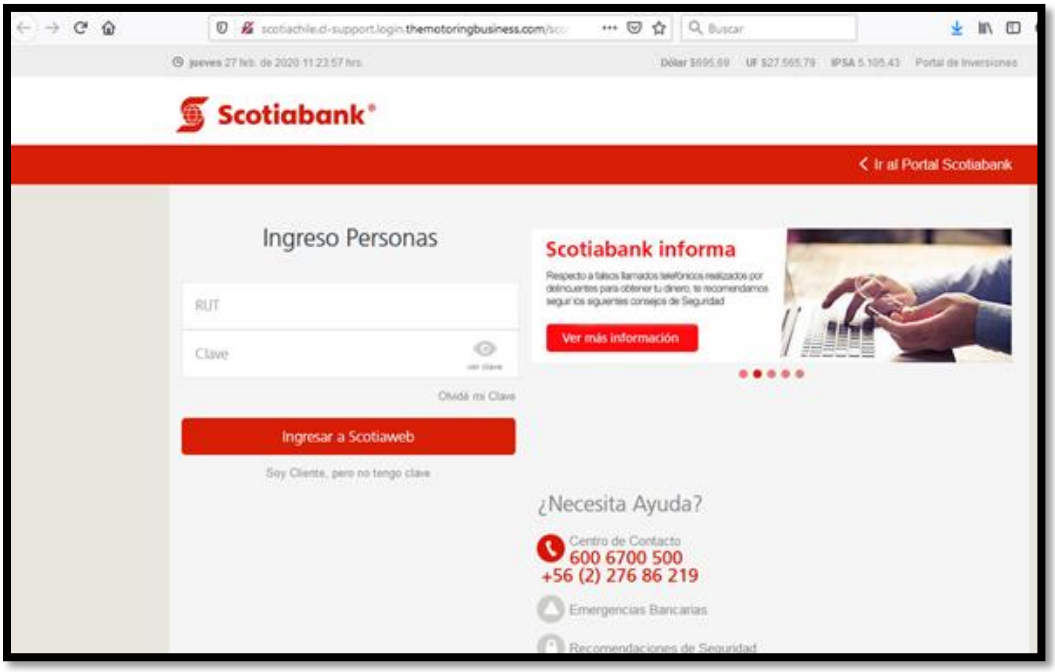


Imagen del sitio



Whois

```
Domain Name: THEMOTORINGBUSINESS.COM
Registry Domain ID: 2058216573_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.launchpad.com
Registrar URL: LaunchPad.com
Updated Date: 2018-08-24T02:27:59Z
Creation Date: 2016-09-08T22:51:31Z
Registrar Registration Expiration Date: 2020-09-08T22:51:31Z
Registrar: Launchpad, Inc. (HostGator)
Registrar IANA ID: 955
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Registry Registrant ID: Not Available From Registry
Registrant Name: Domain Admin
Registrant Organization: Privacy Protect, LLC (PrivacyProtect.org)
Registrant Street: 10 Corporate Drive
Registrant City: Burlington
Registrant State/Province: MA
Registrant Postal Code: 01803
Registrant Country: US
Registrant Phone: +1.8022274003
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: contact@privacyprotect.org
Registry Admin ID: Not Available From Registry
Admin Name: Domain Admin
Admin Organization: Privacy Protect, LLC (PrivacyProtect.org)
Admin Street: 10 Corporate Drive
Admin City: Burlington
Admin State/Province: MA
Admin Postal Code: 01803
Admin Country: US
Admin Phone: +1.8022274003
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: contact@privacyprotect.org
Registry Tech ID: Not Available From Registry
Tech Name: Domain Admin
Tech Organization: Privacy Protect, LLC (PrivacyProtect.org)
Tech Street: 10 Corporate Drive
Tech City: Burlington
Tech State/Province: MA
Tech Postal Code: 01803
Tech Country: US
Tech Phone: +1.8022274003
Tech Phone Ext:
Tech Fax:
Tech Fax Ext:
Tech Email: contact@privacyprotect.org
Name Server: ns8013.hostgator.com
Name Server: ns8014.hostgator.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: 2020.02.28 10:17:15 -03'00'