

Alerta de seguridad informática	8FFR-00115-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	18 de Noviembre de 2019
Última revisión	18 de Noviembre de 2019

NOTIFICACIÓN

La información consignada en el presente informe es producto del análisis de múltiples fuentes, de terceras partes e investigaciones propias del equipo CSIRT. La información contenida en los informes o comunicados está afectada a actualizaciones, por lo cual se recomienda establecer una cuarentena preventiva respecto de los loC 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 loC 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 3 portales fraudulentos asociados a una IP 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

URL Sitio Clonado:

[https://scotiabank\[.\]viewdns\[.\]net/index](https://scotiabank[.]viewdns[.]net/index)

[https://scotiabank\[.\]viewdns\[.\]net/pages/login-form-scotia](https://scotiabank[.]viewdns[.]net/pages/login-form-scotia)

[https://scotiabank\[.\]viewdns\[.\]net/pages/login-form-scotia-empresas](https://scotiabank[.]viewdns[.]net/pages/login-form-scotia-empresas)

Domain scotiabank.viewdns.net			
scotiabank / viewdns / net / Subdomains			
record type	TTL	value	
A	60	144.208.127.32	

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

Certificado

Criteria		Identity = 'scotiabank.viewdns.net'			
Certificates	crt.sh ID	Logged At ↑	Not Before	Not After	Issuer Name
	2108446767	2019-11-13	2019-11-13	2020-02-11	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	2107597583	2019-11-13	2019-11-13	2020-02-11	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

144.208.127.32


Domain scotiabank.viewdns.net is located on IP address << 144.208.127.32 >>	
Block start	144.208.127.0
End of block	144.208.127.255
Block size	256 Domains in block
Block name	SH-335
AS number	395092
Parent block	144.208.0.0 - 144.208.127.255
Organization	Shock Hosting LLC
City	Piscataway
Region/State	New Jersey
Country	 US , United States
Reg. date	2016-04-27
Host name	rdns0.gencorp.review
Domains	1 scotiabank.viewdns.net

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

Localización

Piscataway, New Jersey, Estados Unidos

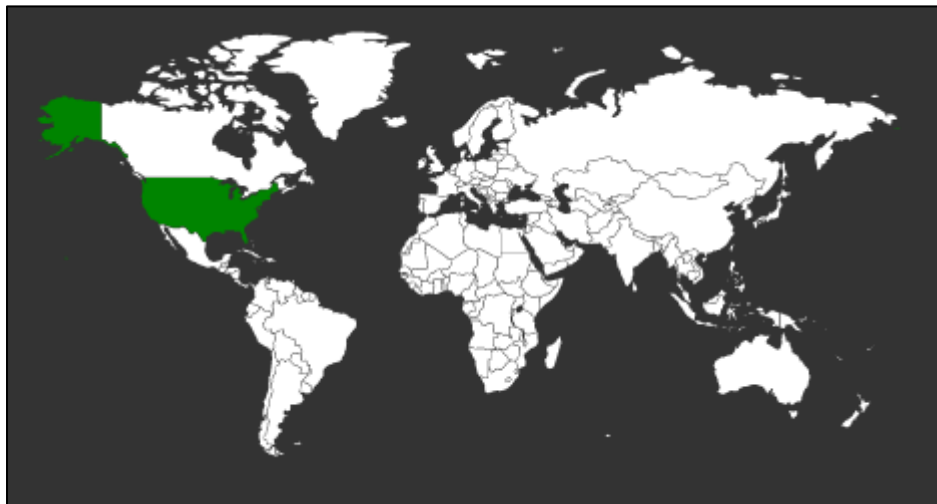
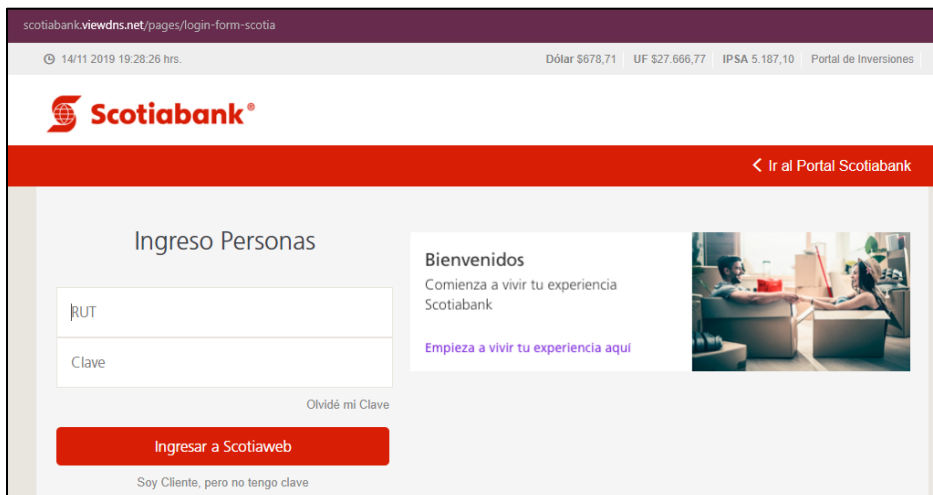
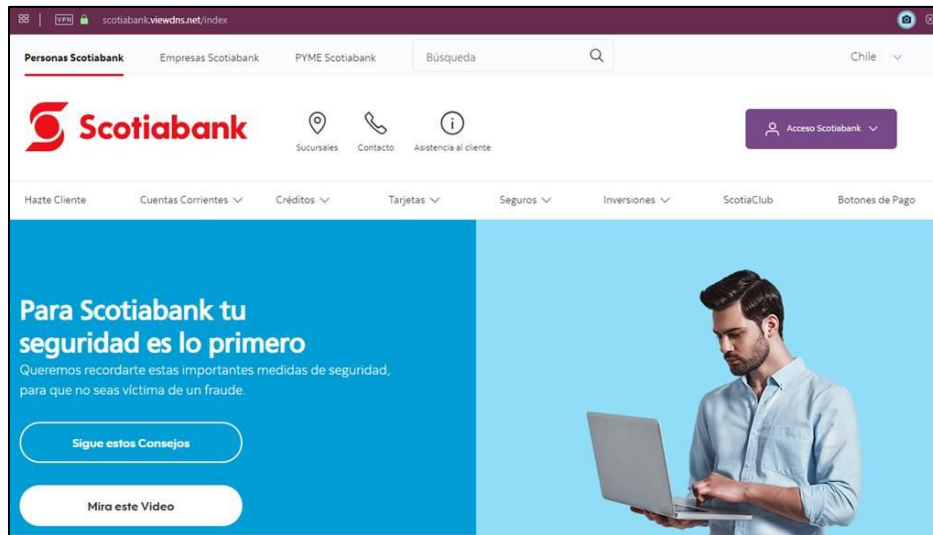


Imagen del sitio



Whois

```
Domain Name: viewdns.net
Registry Domain ID: 1929655284_DOMAIN_NET-VRSN
Registrar WHOIS Server: whois.srsplus.com
Registrar URL: http://srsplus.com
Updated Date: 2017-08-03T20:02:21Z
Creation Date: 2015-05-16T19:28:12Z
Registrar Registration Expiration Date: 2020-05-16T19:28:12Z
Registrar: TLDS LLC, d/b/a SRSPlus
Registrar IANA ID: 320
Reseller:
Domain Status: clientTransferProhibited http://icann.org/epp#clientTransferProhibited
Registry Registrant ID:
Registrant Name: Dan Durrer
Registrant Organization: No-IP.com
Registrant Street: 425 Maestro Dr. Second Floor
Registrant City: Reno
Registrant State/Province: NV
Registrant Postal Code: 89511
Registrant Country: US
Registrant Phone: +1.7758531883
Registrant Phone Ext.:
Registrant Fax:
Registrant Fax Ext.:
Registrant Email: domains@no-ip.com
Registry Admin ID:
Admin Name: Dan Durrer
Admin Organization: No-IP.com
Admin Street: 425 Maestro Dr. Second Floor
Admin City: Reno
Admin State/Province: NV
Admin Postal Code: 89511
Admin Country: US
Admin Phone: +1.7758531883
Admin Phone Ext.:
Admin Fax:
Admin Fax Ext.:
Admin Email: domains@no-ip.com
Registry Tech ID:
Tech Name: Dan Durrer
Tech Organization: No-IP.com
Tech Street: 425 Maestro Dr. Second Floor
Tech City: Reno
Tech State/Province: NV
Tech Postal Code: 89511
Tech Country: US
Tech Phone: +1.7758531883
Tech Phone Ext.:
Tech Fax:
Tech Fax Ext.:
Tech Email: domains@no-ip.com
Name Server: nf2.no-ip.com
Name Server: nf1.no-ip.com
Name Server: nf4.no-ip.com
Name Server: nf3.no-ip.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