Alerta de seguridad informática	8FFR20-00202-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	01 de Febrero de 2020
Última revisión	01 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 dos portales fraudulentos asociados 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-personas-cl-chile[.]cnslv[.]com
scotia-personas-cl-chile[.]cnslv[.]com/BTAM50/login/8QVSE/personas//

Domain cnslv.com

cnslv / com / Subdomains

record type	TTL	value		
A	14400	165.227.16.98		
NS	86400	ns1.mogulbound.io	Zones on DNS server	104.236.38.47
NS	86400	ns2.mogulbound.io	Zones on DNS server	46.101.214.99
MX	14400	0 cnslv.com		
TXT	14400	v=spf1 a mx include:relay.mailchannels.net ?all		
SOA	86400	Mname	ns1.mogulbound.io	
		Rname	mogulbound117.gmail.com	
		Serial number	2020013004	
		Refresh	3600	
		Retry	1800	
		Expire	1209600	
		Minimum TTL	86400	

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

Certificados

Subject DN CN=scotia-personas-cl-chile.cnslv.com
Issuer DN C=US, ST=TX, L=Houston, O=cPanel, Inc., CN=cPanel, Inc. Certification Authority
Serial 357362235967217787418193237430780225 74
Validity 2020-01-30 00:00:00 **to** 2020-04-29 23:59:59 (90 days, 23:59:59)
Names scotia-personas-cl-chile.cnslv.com
www.scotia-personas-cl-chile.cnslv.com

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

IP

165[.]227[.]16[.]98

Domain scotia-personas-cl-chile.cnslv.com is located on IP address
<< 165.227.16.98 >>

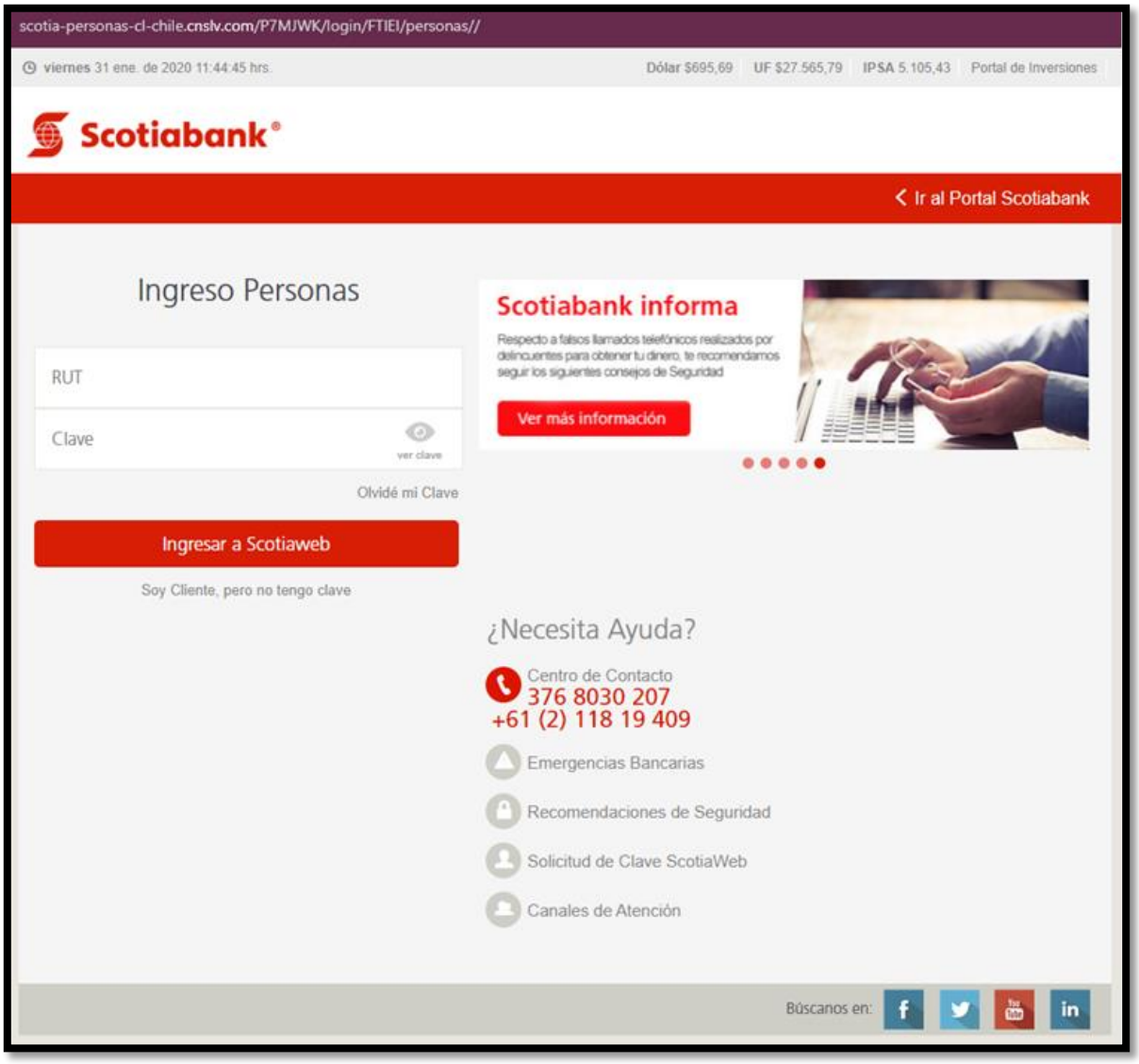
Block start	165.227.0.0
End of block	165.227.255.255
Block size	65536 Domains in block
Block name	SCCI-1-B1
AS number	14061
Parent block	165.0.0.0 - 165.255.255.255
Organization	SantaCruzCommunityInternet
City	New York City
Region/State	New York
Country	US , United States
Reg. date	1993-09-17
Host name	cvps446.serverhostgroup.com
Domains	1 scotia-personas-cl-chile.cnslv.com

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

Localización

Santa Clara, California, Estados Unidos

Imagen del sitio



Whois

```
Domain name: cnslv.com
Registry Domain ID: 2342615659_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.namecheap.com
Registrar URL: http://www.namecheap.com
Updated Date: 2019-11-05T16:50:40.00Z
Creation Date: 2018-12-12T19:13:59.00Z
Registrar Registration Expiration Date: 2020-12-12T19:13:59.00Z
Registrar: NAMECHEAP INC
Registrar IANA ID: 1068
Registrar Abuse Contact Email: abuse@namecheap.com
Registrar Abuse Contact Phone: +1.6613102107
Reseller: NAMECHEAP INC
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Registry Registrant ID:
Registrant Name: WhoisGuard Protected
Registrant Organization: WhoisGuard, Inc.
Registrant Street: P.O. Box 0823-03411
Registrant City: Panama
Registrant State/Province: Panama
Registrant Postal Code:
Registrant Country: PA
Registrant Phone: +507.8365503
Registrant Phone Ext:
Registrant Fax: +51.17057182
Registrant Fax Ext:
Registrant Email: 2c055330a3f04ab1b2dd7efb9c68d4c5.protect@whoisguard.com
Registry Admin ID:
Admin Name: WhoisGuard Protected
Admin Organization: WhoisGuard, Inc.
Admin Street: P.O. Box 0823-03411
Admin City: Panama
Admin State/Province: Panama
Admin Postal Code:
Admin Country: PA
Admin Phone: +507.8365503
Admin Phone Ext:
Admin Fax: +51.17057182
Admin Fax Ext:
Admin Email: 2c055330a3f04ab1b2dd7efb9c68d4c5.protect@whoisguard.com
Registry Tech ID:
Tech Name: WhoisGuard Protected
Tech Organization: WhoisGuard, Inc.
Tech Street: P.O. Box 0823-03411
Tech City: Panama
Tech State/Province: Panama
Tech Postal Code:
Tech Country: PA
Tech Phone: +507.8365503
Tech Phone Ext:
Tech Fax: +51.17057182
Tech Fax Ext:
Tech Email: 2c055330a3f04ab1b2dd7efb9c68d4c5.protect@whoisguard.com
Name Server: ns1.mogulbound.io
Name Server: ns2.mogulbound.io
Name Server: ns3.mogulbound.io
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.