Alerta de seguridad informática	8FFR-00251-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	10 de Marzo de 2020
Última revisión	10 de Marzo 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

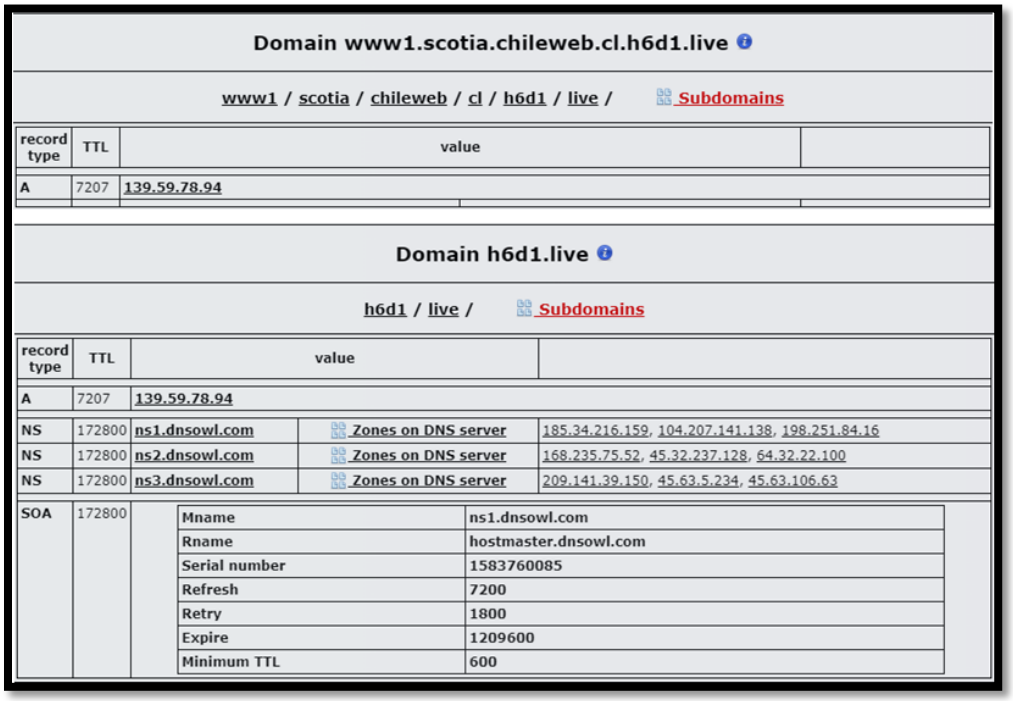
El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de un portal fraudulento asociado a dos IPs que suplanta el sitio web oficial del Banco Scotiabank, el que podría servir para robar credenciales de usuarios de esa entidad.

Lo anterior constituye una falsificación de la marca institucional que podría afectar a usuarios, clientes y a la entidad bancaria aludida.

Indicadores de Compromisos

URL´s

www1[.]scotia[.]chileweb[.]cl[.]h6d1[.]live
www2[.]scotia[.]chileweb[.]cl[.]h6d2[.]live



Domain www1.scotia.chileweb.cl.h6d1.live

www1 / scotia / chileweb / cl / h6d1 / live / Subdomains

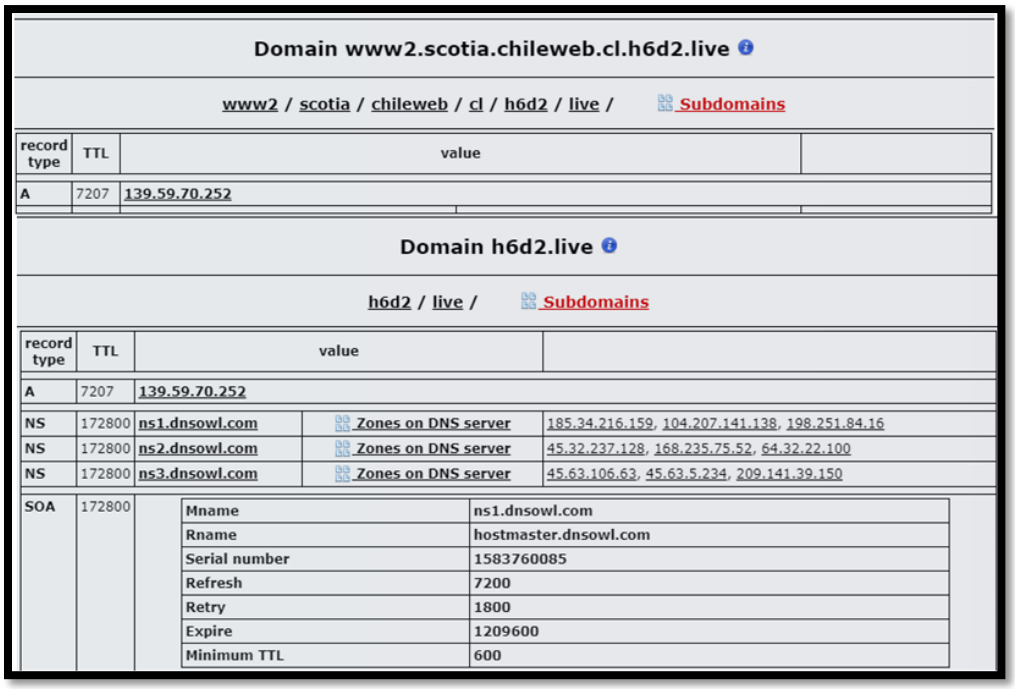
record type	TTL	value	
A	7207	139.59.78.94	

Domain h6d1.live

h6d1 / live / Subdomains

record type	TTL	value		
A	7207	139.59.78.94		
NS	172800	ns1.dnsowl.com	Zones on DNS server	185.34.216.159, 104.207.141.138, 198.251.84.16
NS	172800	ns2.dnsowl.com	Zones on DNS server	168.235.75.52, 45.32.237.128, 64.32.22.100
NS	172800	ns3.dnsowl.com	Zones on DNS server	209.141.39.150, 45.63.5.234, 45.63.106.63

SOA	172800	Mname	ns1.dnsowl.com
		Rname	hostmaster.dnsowl.com
		Serial number	1583760085
		Refresh	7200
		Retry	1800
		Expire	1209600
		Minimum TTL	600



Domain www2.scotia.chileweb.cl.h6d2.live

www2 / scotia / chileweb / cl / h6d2 / live / Subdomains

record type	TTL	value
A	7207	139.59.70.252

Domain h6d2.live

h6d2 / live / Subdomains

record type	TTL	value		
A	7207	139.59.70.252		
NS	172800	ns1.dnsowl.com	Zones on DNS server	185.34.216.159, 104.207.141.138, 198.251.84.16
NS	172800	ns2.dnsowl.com	Zones on DNS server	45.32.237.128, 168.235.75.52, 64.32.22.100
NS	172800	ns3.dnsowl.com	Zones on DNS server	45.63.106.63, 45.63.5.234, 209.141.39.150

SOA	172800	Mname	ns1.dnsowl.com
		Rname	hostmaster.dnsowl.com
		Serial number	1583760085
		Refresh	7200
		Retry	1800
		Expire	1209600
		Minimum TTL	600

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

Certificados

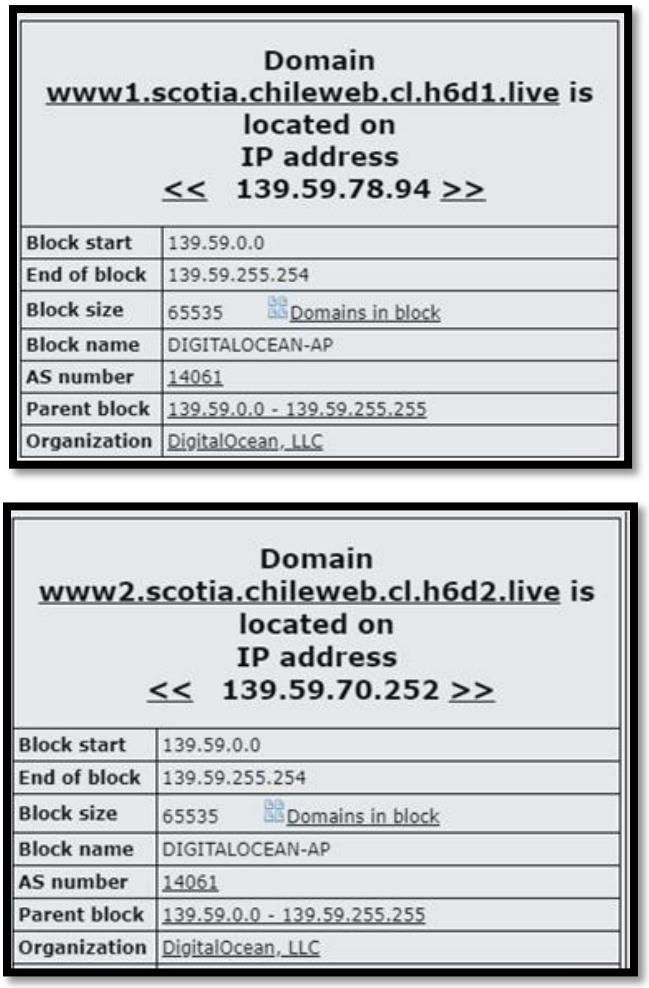
Subject DN	CN=www1.scotia.chileweb.cl.h6d1.live
Issuer DN	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
Serial	3525712839745721668093209701844544174980 41
Validity	2020-03-09 02:34:59 to 2020-06-07 02:34:59 (90 days, 0:00:00)
Names	www1.scotia.chileweb.cl.h6d1.live

Subject DN	CN=www2.scotia.chileweb.cl.h6d2.live
Issuer DN	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
Serial	342913393550460096914072008852432884203471
Validity	2020-03-09 02:34:44 to 2020-06-07 02:34:44 (90 days, 0:00:00)
Names	www2.scotia.chileweb.cl.h6d2.live

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

IP

139[.]59[.]78[.]94
139[.]59[.]70[.]252



Domain www1.scotia.chileweb.cl.h6d1.live is located on IP address << 139.59.78.94 >>

Block start	139.59.0.0
End of block	139.59.255.254
Block size	65535 Domains in block
Block name	DIGITALOCEAN-AP
AS number	14061
Parent block	139.59.0.0 - 139.59.255.255
Organization	DigitalOcean, LLC

Domain www2.scotia.chileweb.cl.h6d2.live is located on IP address << 139.59.70.252 >>

Block start	139.59.0.0
End of block	139.59.255.254
Block size	65535 Domains in block
Block name	DIGITALOCEAN-AP
AS number	14061
Parent block	139.59.0.0 - 139.59.255.255
Organization	DigitalOcean, LLC

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

Localización
Bengaluru, Karnataka, India

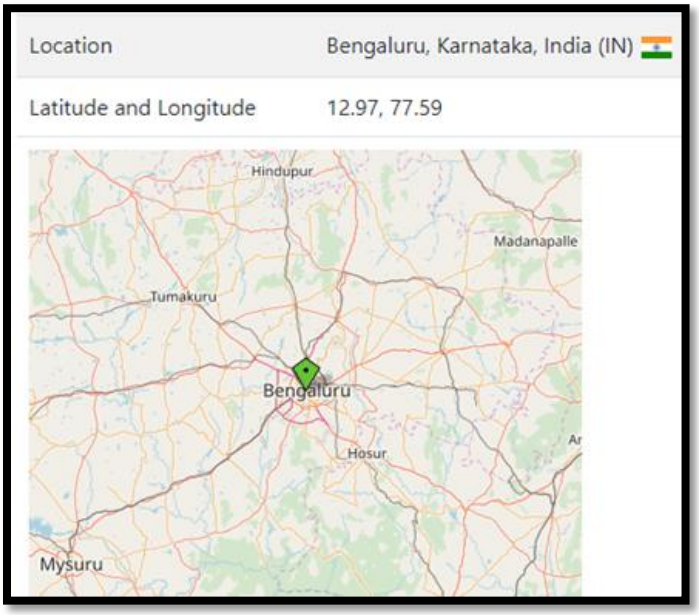
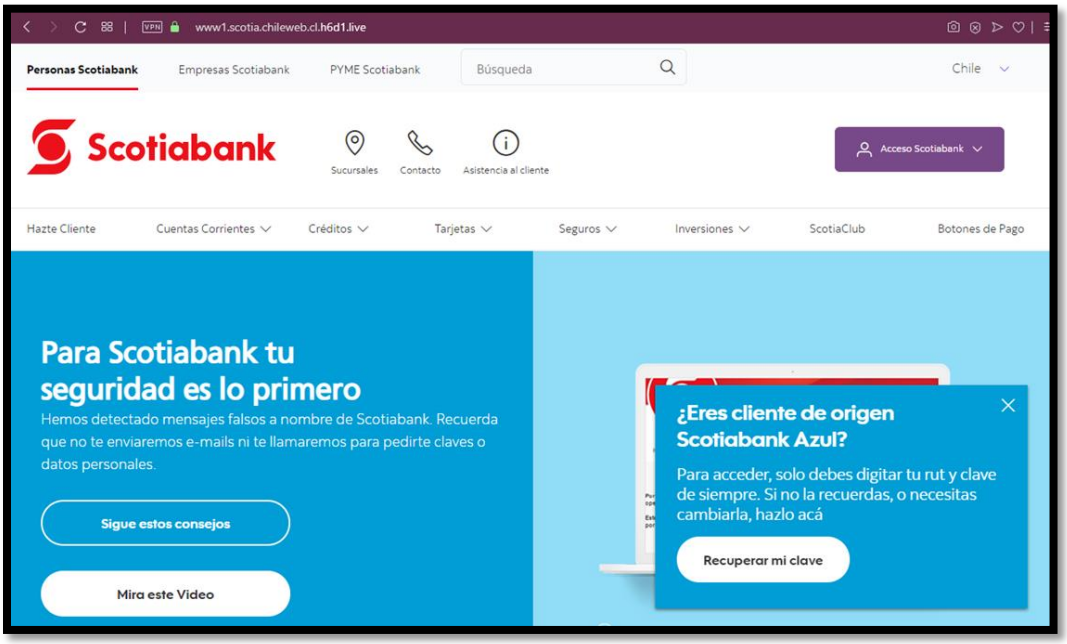
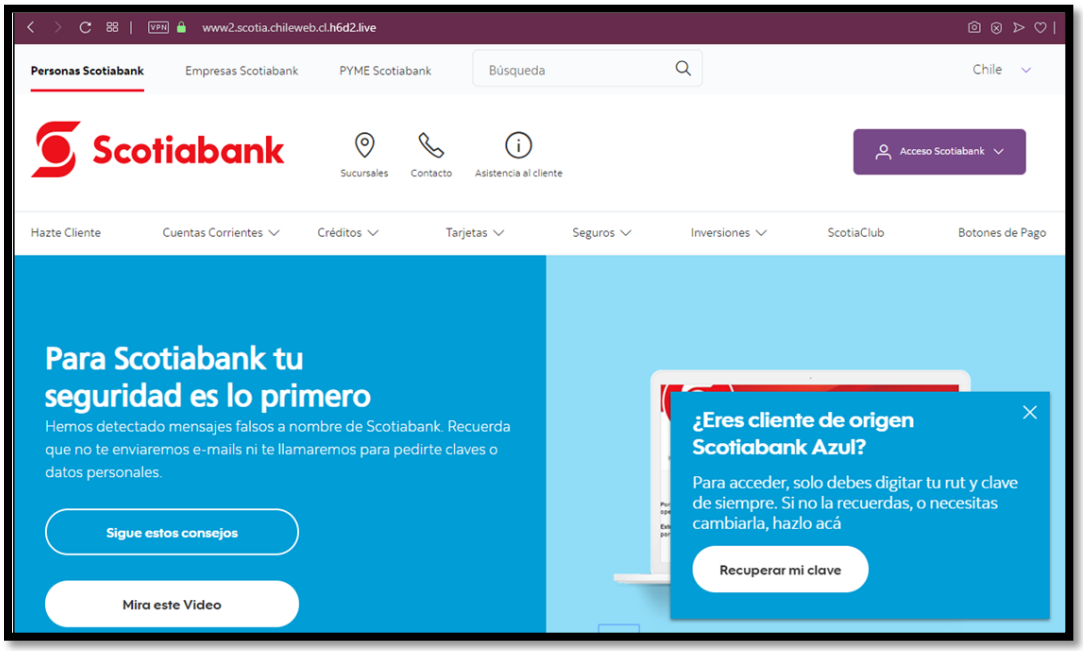


Imagen del sitio





Whois

```
Domain Name: h6dl.live
Registrar WHOIS Server: whois.namesilo.com
Registrar URL: https://www.namesilo.com/
Updated Date: 2020-03-09T07:00:00Z
Creation Date: 2020-03-08T07:00:00Z
Registrar Registration Expiration Date: 2021-03-08T07:00:00Z
Registrar: NameSilo, LLC
Registrar IANA ID: 1479
Registrar Abuse Contact Email: abuse@namesilo.com
Registrar Abuse Contact Phone: +1.4805240066
Domain Status: ok https://www.icann.org/epp#ok
Registry Registrant ID:
Registrant Name: Domain Administrator
Registrant Organization: See PrivacyGuardian.org
Registrant Street: 1928 E. Highland Ave. Ste F104 PMB# 255
Registrant City: Phoenix
Registrant State/Province: AZ
Registrant Postal Code: 85016
Registrant Country: US
Registrant Phone: +1.3478717726
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: pw-8f2562c892dc23c316f414059bb0fd44@privacyguardian.org
Registry Admin ID:
Admin Name: Domain Administrator
Admin Organization: See PrivacyGuardian.org
Admin Street: 1928 E. Highland Ave. Ste F104 PMB# 255
Admin City: Phoenix
Admin State/Province: AZ
Admin Postal Code: 85016
Admin Country: US
Admin Phone: +1.3478717726
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: pw-8f2562c892dc23c316f414059bb0fd44@privacyguardian.org
Registry Tech ID:
Tech Name: Domain Administrator
Tech Organization: See PrivacyGuardian.org
Tech Street: 1928 E. Highland Ave. Ste F104 PMB# 255
Tech City: Phoenix
Tech State/Province: AZ
Tech Postal Code: 85016
Tech Country: US
Tech Phone: +1.3478717726
Tech Phone Ext:
Tech Fax:
Tech Fax Ext:
Tech Email: pw-8f2562c892dc23c316f414059bb0fd44@privacyguardian.org
Name Server: NS1.DNSOWL.COM
Name Server: NS2.DNSOWL.COM
Name Server: NS3.DNSOWL.COM
DNSSEC: unsigned
```

```
Domain Name: h6d2.live
Registrar WHOIS Server: whois.namesilo.com
Registrar URL: https://www.namesilo.com/
Updated Date: 2020-03-09T07:00:00Z
Creation Date: 2020-03-08T07:00:00Z
Registrar Registration Expiration Date: 2021-03-08T07:00:00Z
Registrar: NameSilo, LLC
Registrar IANA ID: 1479
Registrar Abuse Contact Email: abuse@namesilo.com
Registrar Abuse Contact Phone: +1.4805240066
Domain Status: ok https://www.icann.org/epp#ok
Registry Registrant ID:
Registrant Name: Domain Administrator
Registrant Organization: See PrivacyGuardian.org
Registrant Street: 1928 E. Highland Ave. Ste F104 PMB# 255
Registrant City: Phoenix
Registrant State/Province: AZ
Registrant Postal Code: 85016
Registrant Country: US
Registrant Phone: +1.3478717726
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: pw-58ec0960244c429b1040b599f687398e@privacyguardian.org
Registry Admin ID:
Admin Name: Domain Administrator
Admin Organization: See PrivacyGuardian.org
Admin Street: 1928 E. Highland Ave. Ste F104 PMB# 255
Admin City: Phoenix
Admin State/Province: AZ
Admin Postal Code: 85016
Admin Country: US
Admin Phone: +1.3478717726
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: pw-58ec0960244c429b1040b599f687398e@privacyguardian.org
Registry Tech ID:
Tech Name: Domain Administrator
Tech Organization: See PrivacyGuardian.org
Tech Street: 1928 E. Highland Ave. Ste F104 PMB# 255
Tech City: Phoenix
Tech State/Province: AZ
Tech Postal Code: 85016
Tech Country: US
Tech Phone: +1.3478717726
Tech Phone Ext:
Tech Fax:
Tech Fax Ext:
Tech Email: pw-58ec0960244c429b1040b599f687398e@privacyguardian.org
Name Server: NS1.DNSOWL.COM
Name Server: NS2.DNSOWL.COM
Name Server: NS3.DNSOWL.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: 2020.03.10 15:46:02 -03'00'