Alerta de seguridad informática	8FFR20-00206-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	04 de febrero de 2020
Última revisión	04 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 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[.]chile[.]cl[.]n03[.]online
scotia[.]chile[.]cl[.]n03[.]online/portalempresas/
scotia[.]chile[.]cl[.]n03[.]online/login/personas/
scotia[.]chile[.]cl[.]n03[.]online/movil/
scotia[.]chile[.]cl[.]n04[.]online
scotia[.]chile[.]cl[.]n04[.]online/portalempresas/
scotia[.]chile[.]cl[.]n04[.]online/login/personas/
scotia[.]chile[.]cl[.]n04[.]online/movil/

Domain n03.online

n03 / online / Subdomains

record type	TTL	value		
A	7207	134.209.153.89		
NS	172800	ns1.dnsowl.com	Zones on DNS server	198.251.84.16, 185.34.216.159, 104.207.141.138
NS	172800	ns2.dnsowl.com	Zones on DNS server	64.32.22.100, 45.32.237.128, 168.235.75.52
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	1580743848
		Refresh	7200
		Retry	1800
		Expire	1209600
		Minimum TTL	600

Domain n04.online

n04 / online / Subdomains

record type	TTL	value		
A	7207	68.183.94.206		
NS	172800	ns1.dnsowl.com	Zones on DNS server	198.251.84.16, 185.34.216.159, 104.207.141.138
NS	172800	ns2.dnsowl.com	Zones on DNS server	45.32.237.128, 64.32.22.100, 168.235.75.52
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	1580822461
		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=scotia.chile.cl.n03.online
Issuer DN	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
Serial	395330963276367205106304269745060596215425
Validity	2020-01-31 20:02:33 **to** 2020-04-30 20:02:33 (90 days, 0:00:00)
Names	scotia.chile.cl.n03.online

Subject DN	CN=scotia.chile.cl.n04.online
Issuer DN	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
Serial	263680107365239528541914586322875619657205
Validity	2020-02-04 00:57:40 **to** 2020-05-04 00:57:40 (90 days, 0:00:00)
Names	scotia.chile.cl.n04.online

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

IP

134[.]209[.]153[.]89

68[.]183[.]94[.]206

Domain scotia.chile.cl.n03.online is located on IP address << 134.209.153.89 >>

Block start	134.209.0.0
End of block	134.209.255.255
Block size	65536 Domains in block
Block name	COV-HC-NET134
AS number	14061
Parent block	134.0.0.0 - 134.255.255.255
Organization	COVIDIENLP
City	Mansfield
Region/State	Massachusetts
Country	US , United States
Reg. date	1989-07-24
Host name	no record in reverse zone
Domains	1 scotia.chile.cl.n03.online

Domain scotia.chile.cl.n04.online is located on IP address << 68.183.94.206 >>

Block start	68.183.0.0
End of block	68.183.255.255
Block size	65536 Domains in block
Block name	DSLEXTREME-NWK-6
AS number	14061
Parent block	68.0.0.0 - 68.255.255.255
Organization	DSL Extreme
City	Chatsworth
Region/State	California
Country	US , United States
Reg. date	2005-04-14
Host name	no record in reverse zone
Domain count	>= 4 Servers around
Domains	1 n01.online 2 n04.online 3 scotia.chile.cl.n01.online 4 scotia.chile.cl.n04.online

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

Localización

India, Bangalore, Karnataka

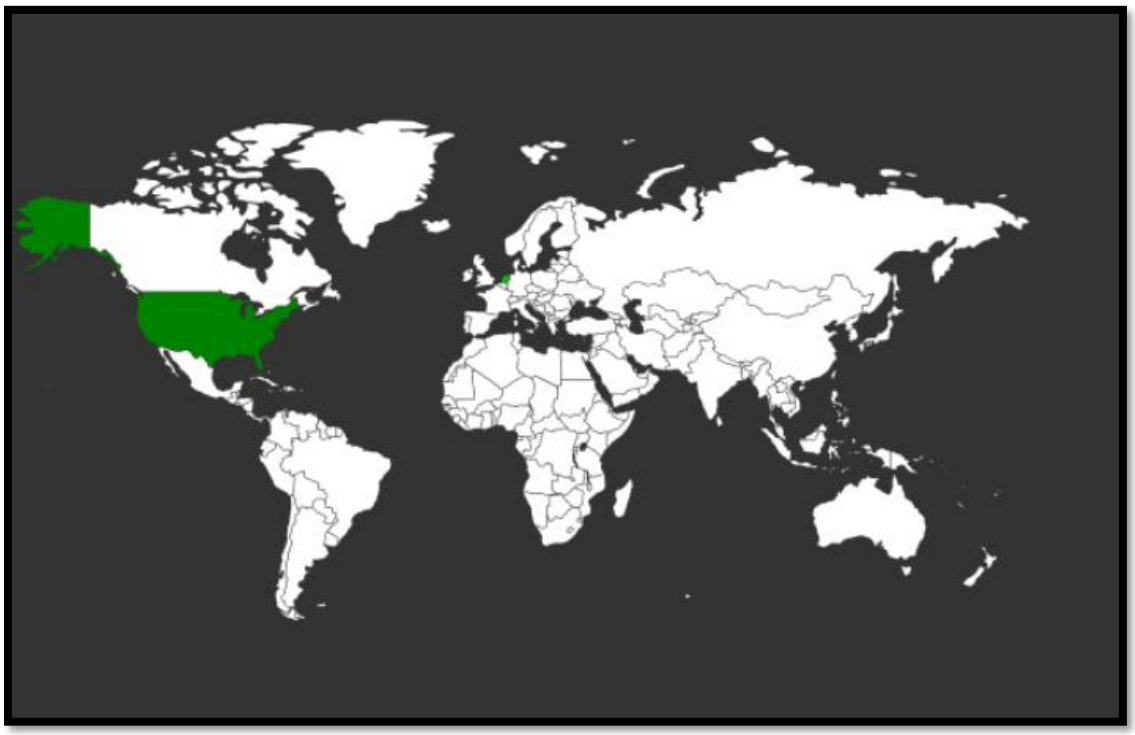
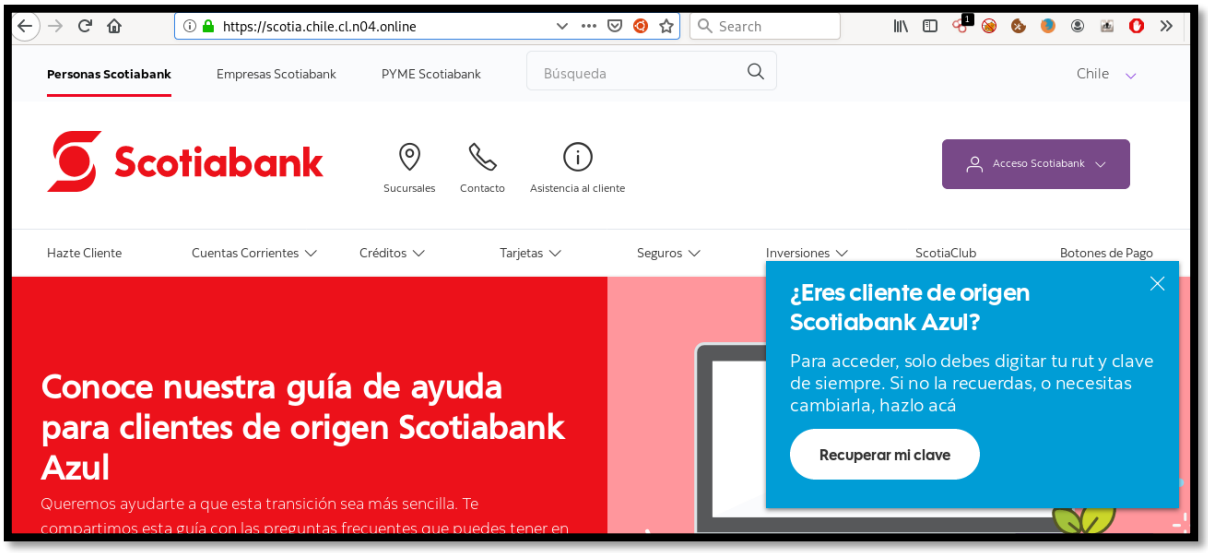


Imagen del sitio



Whois

```
Domain Name: N03.ONLINE
Registry Domain ID: D169033461-CNIC
Registrar WHOIS Server: whois.namesilo.com
Registrar URL: https://www.namesilo.com
Updated Date: 2020-01-31T20:45:36.0Z
Creation Date: 2020-01-31T20:32:40.0Z
Registry Expiry Date: 2021-01-31T23:59:59.0Z
Registrar: NameSilo, LLC
Registrar IANA ID: 1479
Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: addPeriod https://icann.org/epp#addPeriod
Registrant Organization: See PrivacyGuardian.org
Registrant State/Province: AZ
Registrant Country: US
Registrant Email: Please query the RDDS service of the Registrar of Record identified in this output for infor
mation on how to contact the Registrant, Admin, or Tech contact of the queried domain name.
Admin Email: Please query the RDDS service of the Registrar of Record identified in this output for informatio
n on how to contact the Registrant, Admin, or Tech contact of the queried domain name.
Tech Email: Please query the RDDS service of the Registrar of Record identified in this output for information
 on how to contact the Registrant, Admin, or Tech contact of the queried domain name.
Name Server: NS1.DNSOWL.COM
Name Server: NS2.DNSOWL.COM
Name Server: NS3.DNSOWL.COM
DNSSEC: unsigned
```

```
Domain Name: N04.ONLINE
Registry Domain ID: D169433906-CNIC
Registrar WHOIS Server: whois.namesilo.com
Registrar URL: https://www.namesilo.com
Updated Date: 2020-02-04T01:00:23.0Z
Creation Date: 2020-02-04T00:51:51.0Z
Registry Expiry Date: 2021-02-04T23:59:59.0Z
Registrar: NameSilo, LLC
Registrar IANA ID: 1479
Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: addPeriod https://icann.org/epp#addPeriod
Registrant Organization: See PrivacyGuardian.org
Registrant State/Province: AZ
Registrant Country: US
Registrant Email: Please query the RDDS service of the Registrar of Record identified in this output for infor
mation on how to contact the Registrant, Admin, or Tech contact of the queried domain name.
Admin Email: Please query the RDDS service of the Registrar of Record identified in this output for informatio
n on how to contact the Registrant, Admin, or Tech contact of the queried domain name.
Tech Email: Please query the RDDS service of the Registrar of Record identified in this output for information
 on how to contact the Registrant, Admin, or Tech contact of the queried domain name.
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: 2020.02.04 20:44:17 -03'00'