Alerta de seguridad informática	8FFR20-00203-01
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

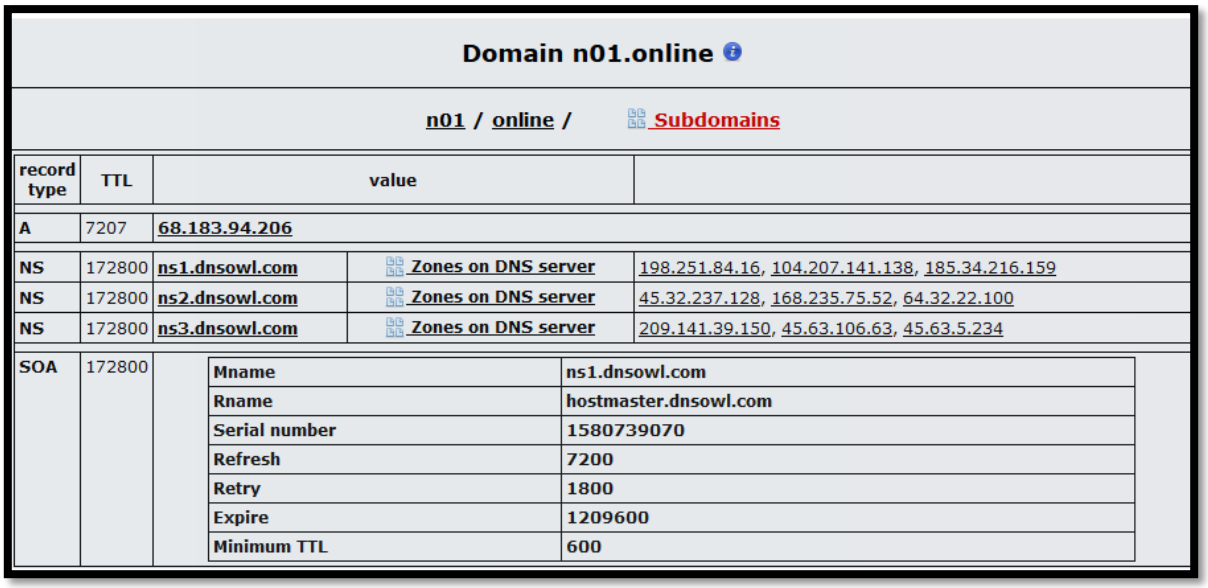
El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de un portal fraudulento asociado a una IP que suplanta el sitio web oficial de Banco Scotiabank, el que podría servir para robar credenciales de usuarios de esa entidad.

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[.]n01[.]online
scotia[.]chile[.]cl[.]n01[.]online/portalempresas/
scotia[.]chile[.]cl[.]n01[.]online/login/personas/
scotia[.]chile[.]cl[.]n01[.]online/movil/
scotia[.]chile[.]cl[.]n02[.]online/portalempresas/
scotia[.]chile[.]cl[.]n02[.]online/login/personas/
scotia[.]chile[.]cl[.]n02[.]online/movil/
scotiablakclpersonasfbancenlinea[.]kenjiglobal[.]com/36OJOE/login/Y4VFQ/personas//

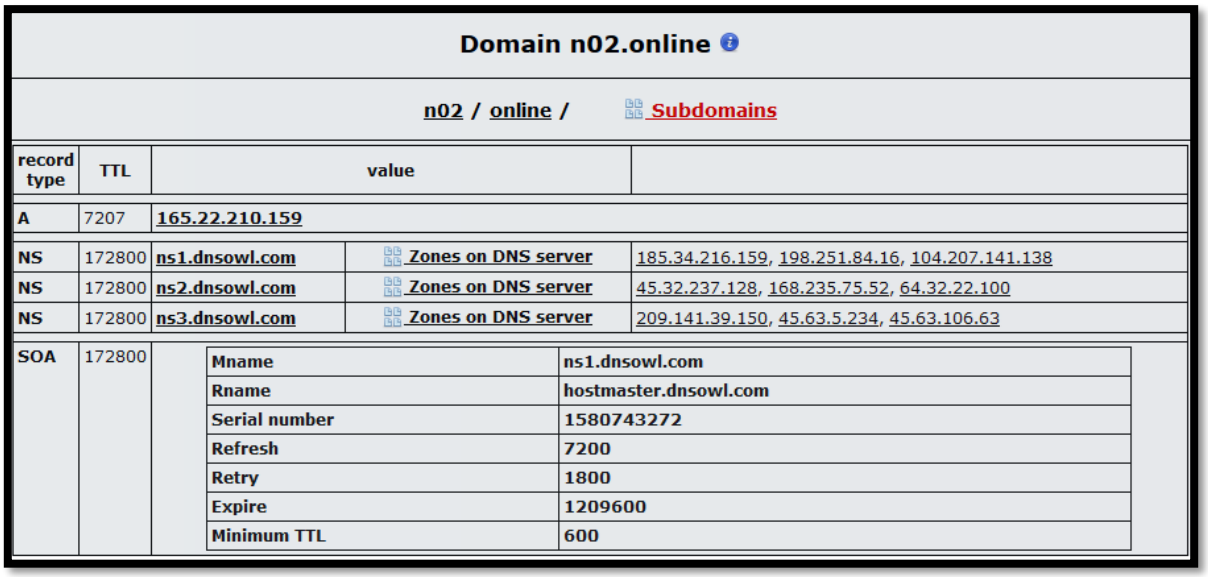


Domain n01.online

n01 / 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, 104.207.141.138, 185.34.216.159
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	209.141.39.150, 45.63.106.63, 45.63.5.234

SOA	172800	Mname	ns1.dnsowl.com
		Rname	hostmaster.dnsowl.com
		Serial number	1580739070
		Refresh	7200
		Retry	1800
		Expire	1209600
		Minimum TTL	600



Domain n02.online

n02 / online / Subdomains

record type	TTL	value		
A	7207	165.22.210.159		
NS	172800	ns1.dnsowl.com	Zones on DNS server	185.34.216.159, 198.251.84.16, 104.207.141.138
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	209.141.39.150, 45.63.5.234, 45.63.106.63

SOA	172800	Mname	ns1.dnsowl.com
		Rname	hostmaster.dnsowl.com
		Serial number	1580743272
		Refresh	7200
		Retry	1800
		Expire	1209600
		Minimum TTL	600

Domain scotiablakclpersonasfbancenlinea.kenjiglobal.com

scotiablakclpersonasfbancenlinea / kenjiglobal / com / Subdomains

record type	TTL	value
A	14400	119.81.10.24

Domain kenjiglobal.com

kenjiglobal / com / Subdomains

record type	TTL	value		
A	14400	119.81.10.24		
NS	86400	ns2.tiwilee.com	Zones on DNS server	119.81.10.25
NS	86400	ns1.tiwilee.com	Zones on DNS server	119.81.10.24
MX	14400	10 mx.zoho.com		204.141.42.121
MX	14400	20 mx2.zoho.com		204.141.42.121
TXT	600	v=spf1 ip4:216.12.199.232 ip4:119.81.10.24 include:zoho.com ~all		
SOA	86400	Mname: ns1.tiwilee.com Rname: myname.tiwilee.com Serial number: 2019121701 Refresh: 3600 Retry: 7200 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.chile.cl.n01.online
Issuer DN	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
Serial	336150688199120118124721338219433263107403
Validity	2020-01-31 18:44:14 **to** 2020-04-30 18:44:14 (90 days, 0:00:00)
Names	scotia.chile.cl.n01.online

Subject DN	CN=scotia.chile.cl.n02.online
Issuer DN	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
Serial	311466328548568490303145170130783310480224
Validity	2020-01-31 18:44:17 **to** 2020-04-30 18:44:17 (90 days, 0:00:00)
Names	scotia.chile.cl.n02.online

Subject DN	CN=scotiablakclpersonasfbancenlinea.kenjiglobal.com
Issuer DN	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
Serial	346208650163067757720416271145746647725105
Validity	2020-01-31 17:03:14 **to** 2020-04-30 17:03:14 (90 days, 0:00:00)
Names	scotiablakclpersonasfbancenlinea.kenjiglobal.com www.scotiablakclpersonasfbancenlinea.kenjiglobal.com

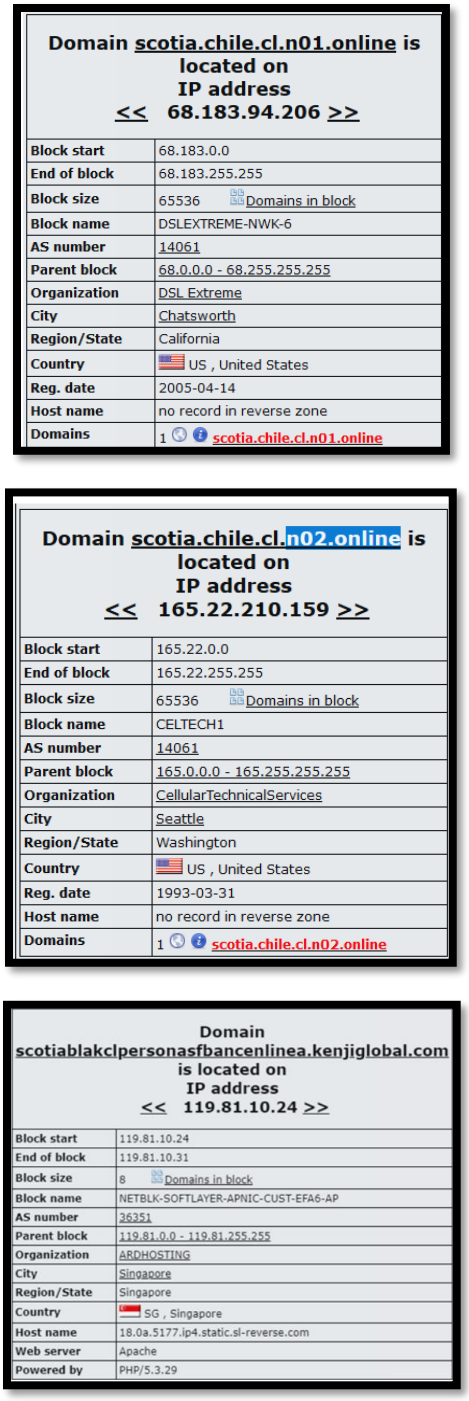
Ilustración 2 Certificado Utilizado en Url del sitio Falso del Banco Scotiabank.

IP

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

165[.]22[.]210[.]159

119[.]81[.]10[.]24



Domain scotia.chile.cl.n01.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
Domains	1 scotia.chile.cl.n01.online

Domain scotia.chile.cl.n02.online is located on IP address << 165.22.210.159 >>

Block start	165.22.0.0
End of block	165.22.255.255
Block size	65536 Domains in block
Block name	CELTECH1
AS number	14061
Parent block	165.0.0.0 - 165.255.255.255
Organization	CellularTechnicalServices
City	Seattle
Region/State	Washington
Country	US , United States
Reg. date	1993-03-31
Host name	no record in reverse zone
Domains	1 scotia.chile.cl.n02.online

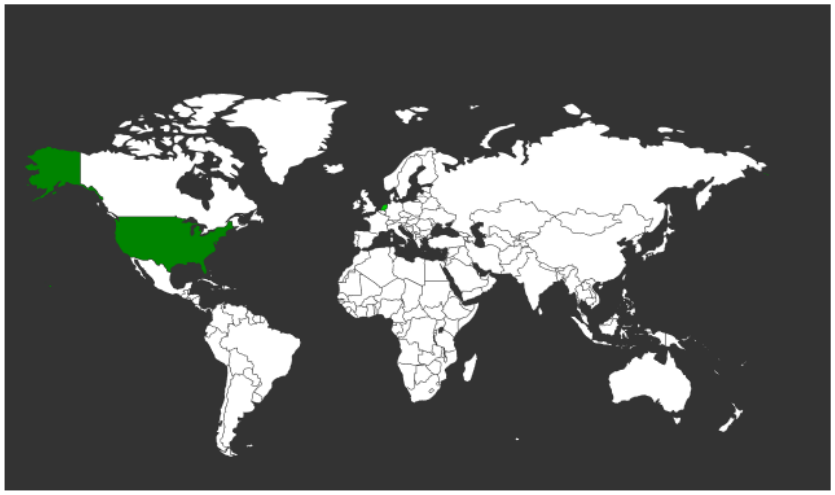
Domain scotiablakclpersonasfbancenlinea.kenjiglobal.com is located on IP address << 119.81.10.24 >>

Block start	119.81.10.24
End of block	119.81.10.31
Block size	8 Domains in block
Block name	NETBLK-SOFTLAYER-APNIC-CUST-EFA6-AP
AS number	36351
Parent block	119.81.0.0 - 119.81.255.255
Organization	ARDHOSTING
City	Singapore
Region/State	Singapore
Country	SG , Singapore
Host name	18.0a.5177.ip4.static.sl-reverse.com
Web server	Apache
Powered by	PHP/5.3.29

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

Localización

India, Bangalore, Karnataka



Singapore, Singapore

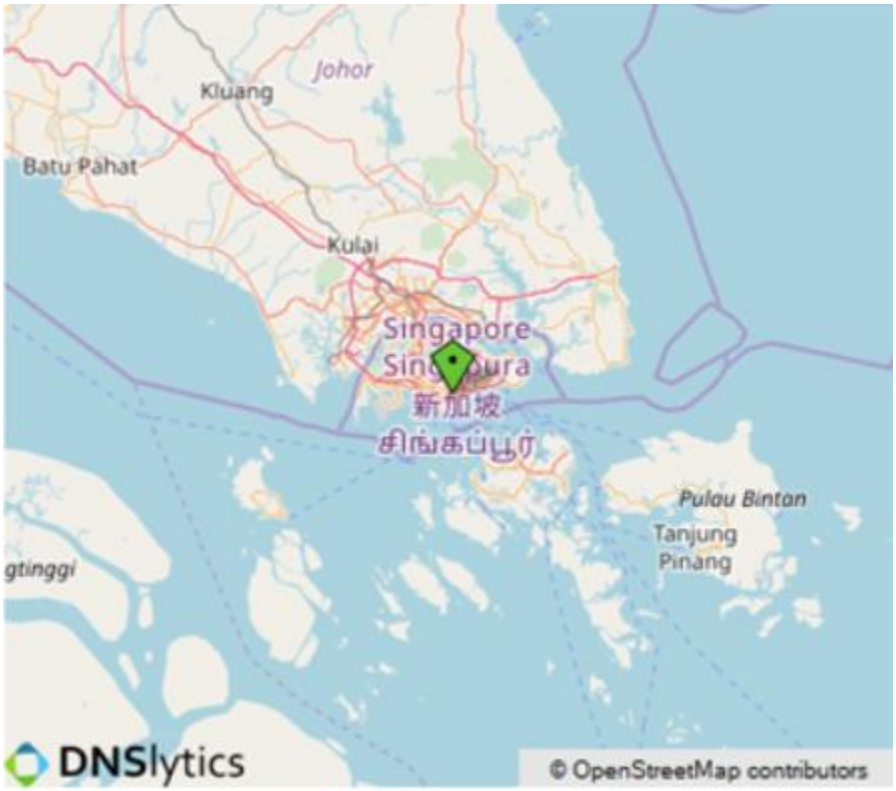
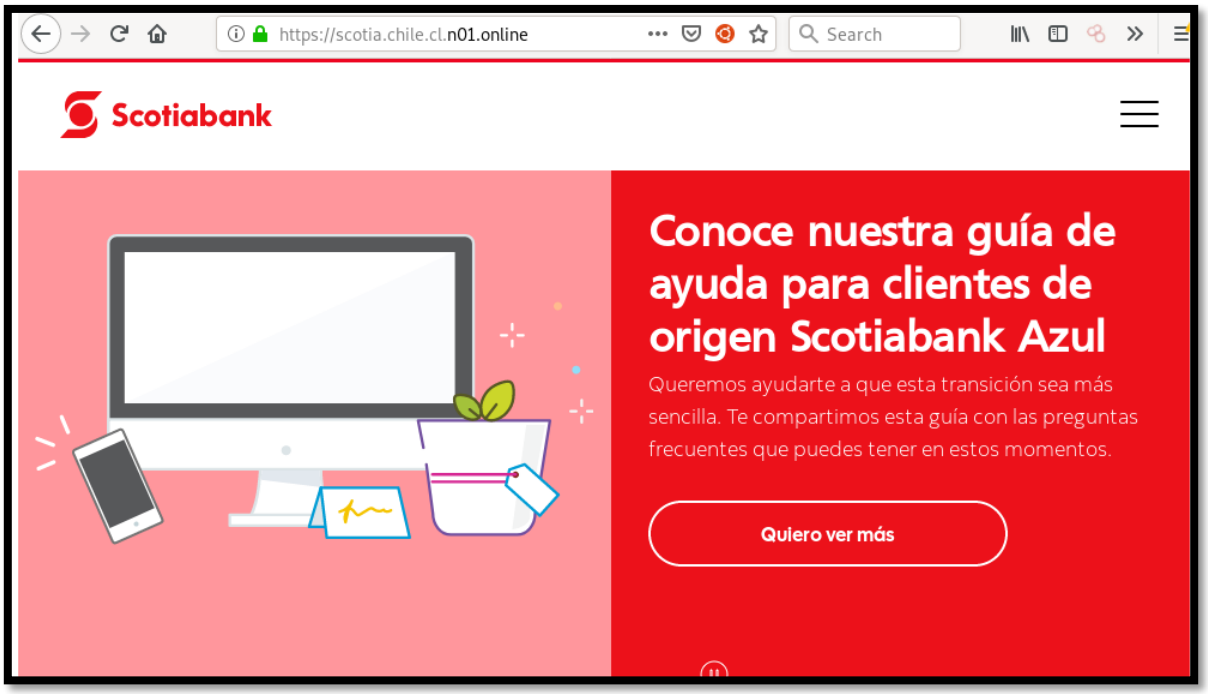
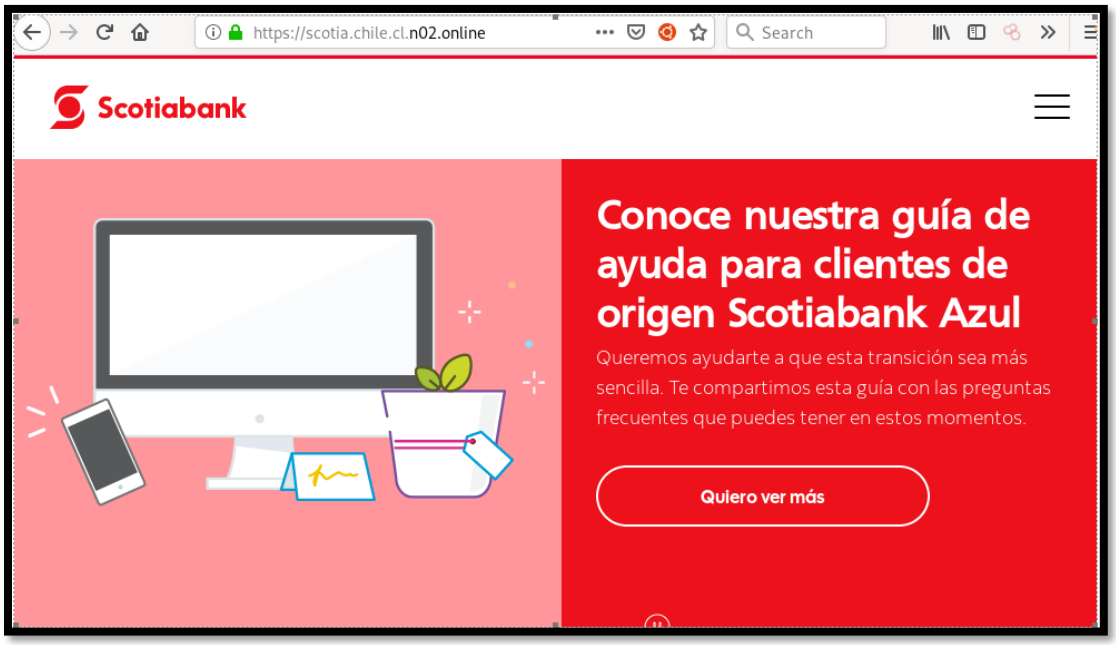
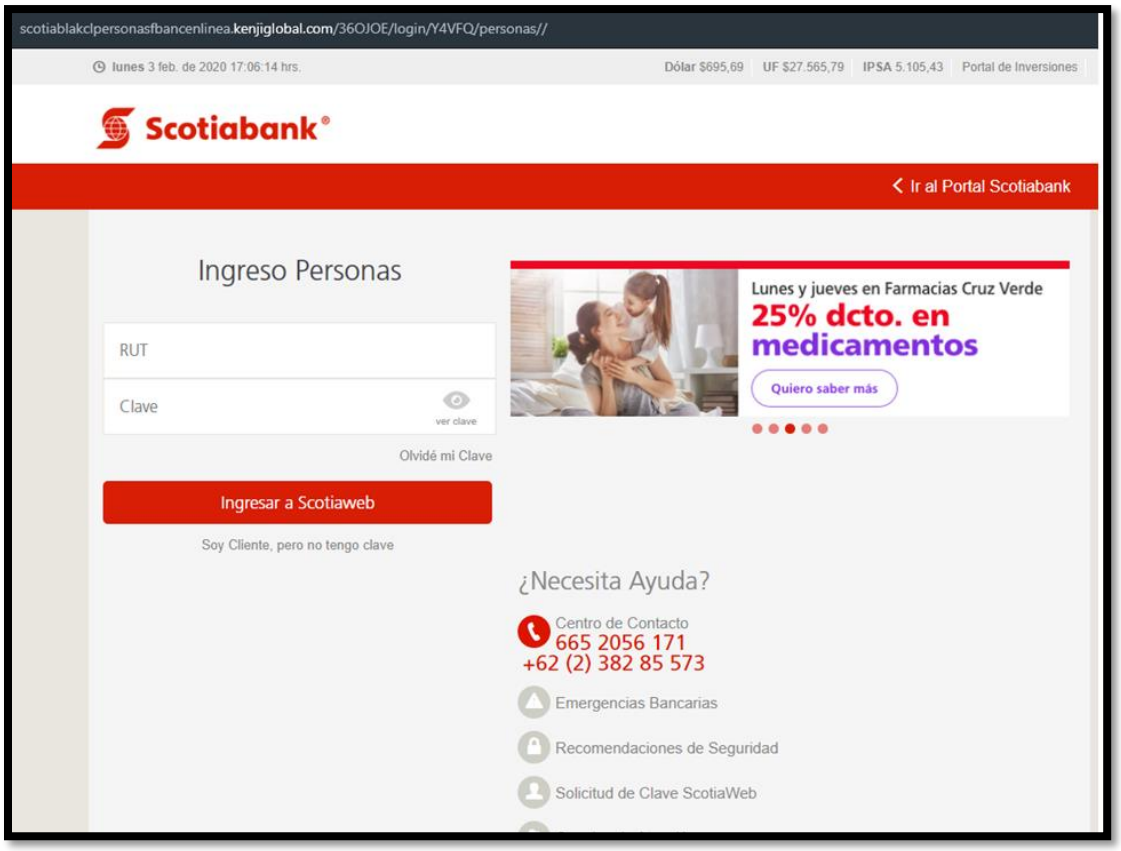


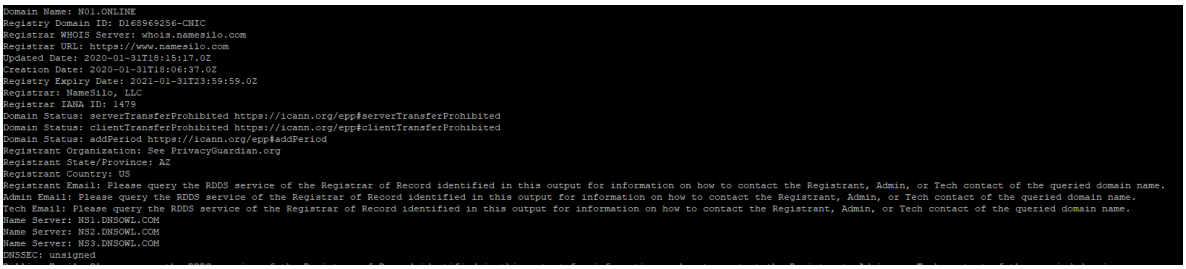
Imagen del sitio



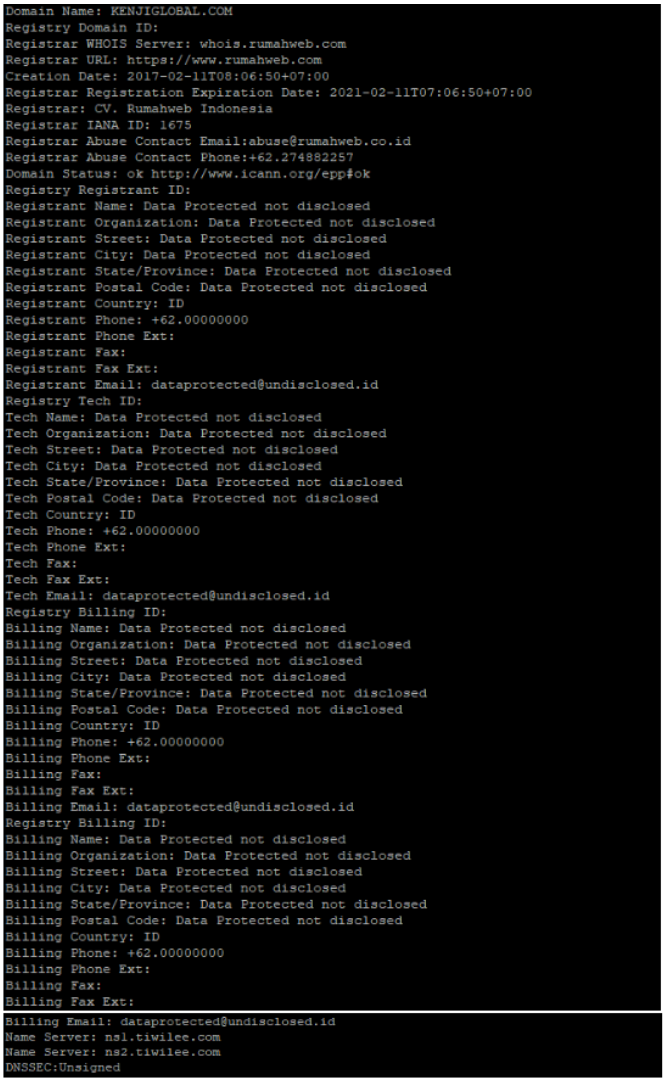



scotiablakclpersonasfbancenlinea.kenjiglobal.com/36OJOE/login/Y4VFQ/personas//
lunes 3 feb. de 2020 17:06:14 hrs.
Dólar $695,69
UF $27.565,79
IPSA 5.105,43
Portal de Inversiones
Scotiabank
Ir al Portal Scotiabank
Ingreso Personas
RUT
Clave
ver clave
Olvidé mi Clave
Ingresar a Scotiaweb
Soy Cliente, pero no tengo clave
Lunes y jueves en Farmacias Cruz Verde
25% dcto. en medicamentos
Quiero saber más
¿Necesita Ayuda?
Centro de Contacto
665 2056 171
+62 (2) 382 85 573
Emergencias Bancarias
Recomendaciones de Seguridad
Solicitud de Clave ScotiaWeb

Whois


Domain Name: N01.ONLINE
Registry Domain ID: D168969256-CNIC
Registrar WHOIS Server: whois.namesilo.com
Registrar URL: https://www.namesilo.com
Updated Date: 2020-01-31T18:15:17.0Z
Creation Date: 2020-01-31T18:06:37.0Z
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 information 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 information 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: N02.ONLINE
Registry Domain ID: D168969261-CNIC
Registrar WHOIS Server: whois.namesilo.com
Registrar URL: https://www.namesilo.com
Updated Date: 2020-01-31T18:15:12.0Z
Creation Date: 2020-01-31T18:06:37.0Z
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 information 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 information 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: KENJIGLOBAL.COM
Registry Domain ID:
Registrar WHOIS Server: whois.rumahweb.com
Registrar URL: https://www.rumahweb.com
Creation Date: 2017-02-11T08:06:50+07:00
Registrar Registration Expiration Date: 2021-02-11T07:06:50+07:00
Registrar: CV. Rumahweb Indonesia
Registrar IANA ID: 1675
Registrar Abuse Contact Email:abuse@rumahweb.co.id
Registrar Abuse Contact Phone:+62.274882257
Domain Status: ok http://www.icann.org/epp#ok
Registry Registrant ID:
Registrant Name: Data Protected not disclosed
Registrant Organization: Data Protected not disclosed
Registrant Street: Data Protected not disclosed
Registrant City: Data Protected not disclosed
Registrant State/Province: Data Protected not disclosed
Registrant Postal Code: Data Protected not disclosed
Registrant Country: ID
Registrant Phone: +62.00000000
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: dataprotected@undisclosed.id
Registry Tech ID:
Tech Name: Data Protected not disclosed
Tech Organization: Data Protected not disclosed
Tech Street: Data Protected not disclosed
Tech City: Data Protected not disclosed
Tech State/Province: Data Protected not disclosed
Tech Postal Code: Data Protected not disclosed
Tech Country: ID
Tech Phone: +62.00000000
Tech Phone Ext:
Tech Fax:
Tech Fax Ext:
Tech Email: dataprotected@undisclosed.id
Registry Billing ID:
Billing Name: Data Protected not disclosed
Billing Organization: Data Protected not disclosed
Billing Street: Data Protected not disclosed
Billing City: Data Protected not disclosed
Billing State/Province: Data Protected not disclosed
Billing Postal Code: Data Protected not disclosed
Billing Country: ID
Billing Phone: +62.00000000
Billing Phone Ext:
Billing Fax:
Billing Fax Ext:
Billing Email: dataprotected@undisclosed.id
Registry Billing ID:
Billing Name: Data Protected not disclosed
Billing Organization: Data Protected not disclosed
Billing Street: Data Protected not disclosed
Billing City: Data Protected not disclosed
Billing State/Province: Data Protected not disclosed
Billing Postal Code: Data Protected not disclosed
Billing Country: ID
Billing Phone: +62.00000000
Billing Phone Ext:
Billing Fax:
Billing Fax Ext:
Billing Email: dataprotected@undisclosed.id
Name Server: ns1.tiwilee.com
Name Server: ns2.tiwilee.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 09:41:21 -03'00'