Ministerio del Interior y Seguridad Pública

Gobierno de Chile

Alerta de Seguridad Cibernética

CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

Alerta de seguridad cibernética	8FFR20-00340-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	16 de abril de 2020
Última revisión	16 de abril 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 tres portales fraudulentos asociados a tres IPs que suplantan el sitio web oficial de Banco Scotiabank, el que podría servir para robar credenciales de usuarios de esa entidad.

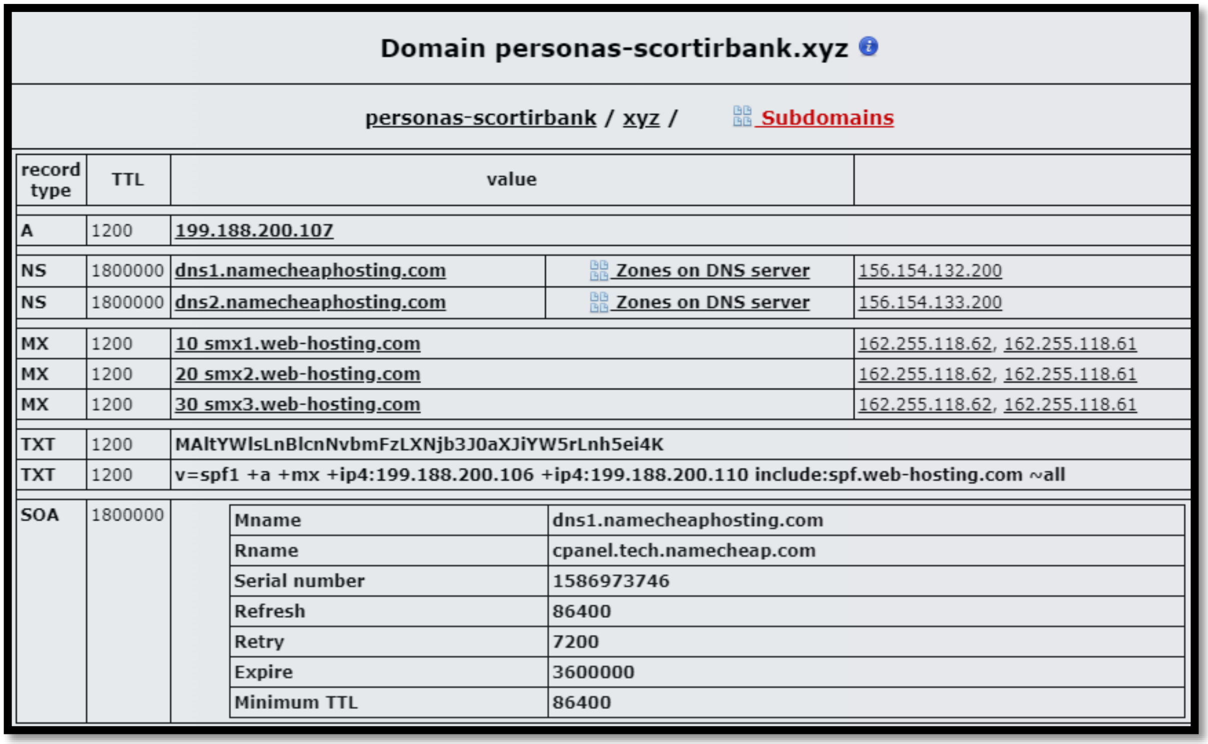
Lo anterior constituye una falsificación de la marca institucional que podría afectar a usuarios, clientes y a la entidad bancaria aludida.

INDICADORES DE COMPROMISO

URL
personas-scortirbank[.]xyz
loginspersnas-scortiarbarnk-cl[.]xyz
pre-covid[.]info

IP
199[.]188[.]200[.]107
104[.]219[.]248[.]113
178[.]159[.]36[.]139

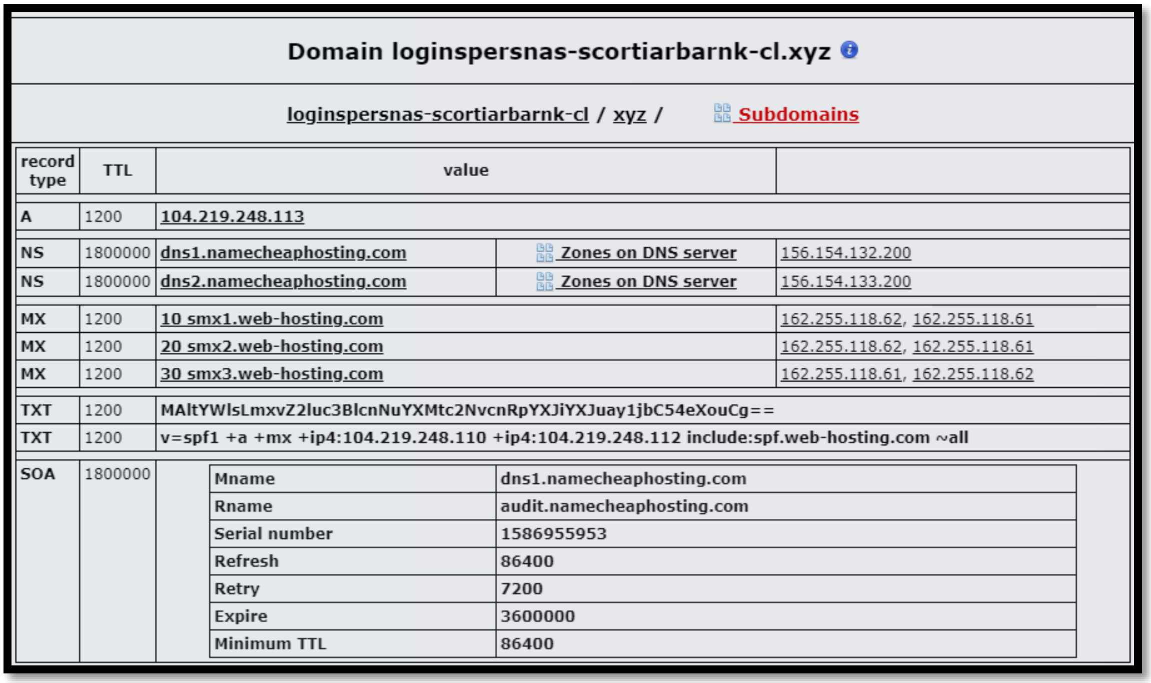
DOMINIOS DONDE SE ALOJA URL



Domain personas-scortirbank.xyz

personas-scortirbank / xyz / Subdomains

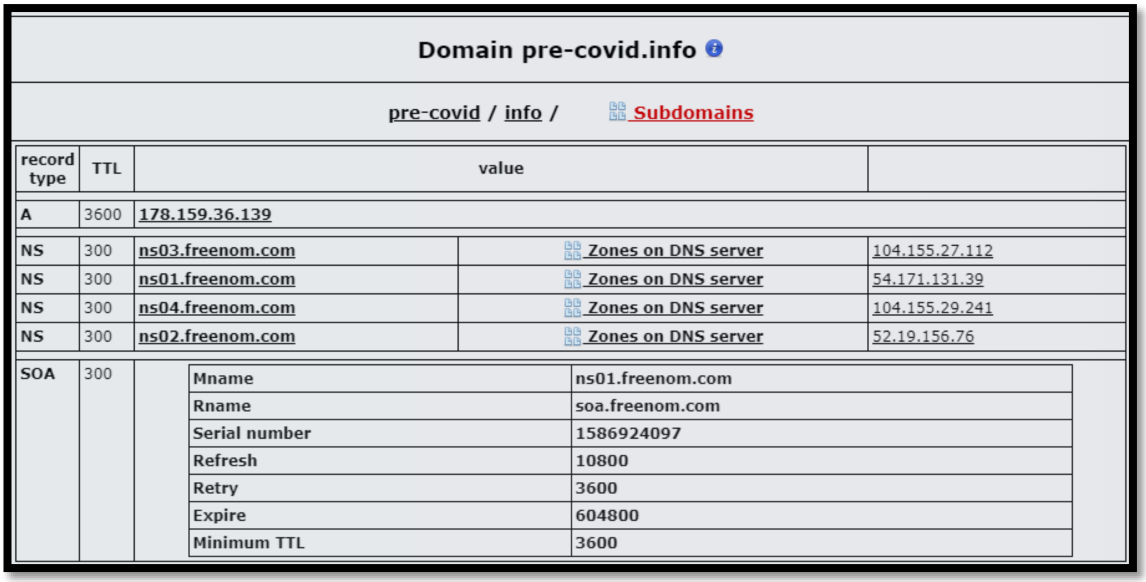
record type	TTL	value		
A	1200	199.188.200.107		
NS	1800000	dns1.namecheaphosting.com	Zones on DNS server	156.154.132.200
NS	1800000	dns2.namecheaphosting.com	Zones on DNS server	156.154.133.200
MX	1200	10 smx1.web-hosting.com		162.255.118.62, 162.255.118.61
MX	1200	20 smx2.web-hosting.com		162.255.118.62, 162.255.118.61
MX	1200	30 smx3.web-hosting.com		162.255.118.62, 162.255.118.61
TXT	1200	MAltYWlsLnBlcnNvbmFzLXNjb3J0aXJiYW5rLnh5ei4K		
TXT	1200	v=spf1 +a +mx +ip4:199.188.200.106 +ip4:199.188.200.110 include:spf.web-hosting.com ~all		
SOA	1800000	Mname	dns1.namecheaphosting.com	
		Rname	cpanel.tech.namecheap.com	
		Serial number	1586973746	
		Refresh	86400	
		Retry	7200	
		Expire	3600000	
		Minimum TTL	86400	



Domain loginspersnas-scortiarbarnk-cl.xyz

loginspersnas-scortiarbarnk-cl / xyz / Subdomains

record type	TTL	value		
A	1200	104.219.248.113		
NS	1800000	dns1.namecheaphosting.com	Zones on DNS server	156.154.132.200
NS	1800000	dns2.namecheaphosting.com	Zones on DNS server	156.154.133.200
MX	1200	10 smx1.web-hosting.com		162.255.118.62, 162.255.118.61
MX	1200	20 smx2.web-hosting.com		162.255.118.62, 162.255.118.61
MX	1200	30 smx3.web-hosting.com		162.255.118.61, 162.255.118.62
TXT	1200	MAltYWlsLmxvZ2luc3BlcnNuYXMtc2NvcnRpYXJiYXJuay1jbC54eXouCg==		
TXT	1200	v=spf1 +a +mx +ip4:104.219.248.110 +ip4:104.219.248.112 include:spf.web-hosting.com ~all		
SOA	1800000	Mname	dns1.namecheaphosting.com	
		Rname	audit.namecheaphosting.com	
		Serial number	1586955953	
		Refresh	86400	
		Retry	7200	
		Expire	3600000	
		Minimum TTL	86400	

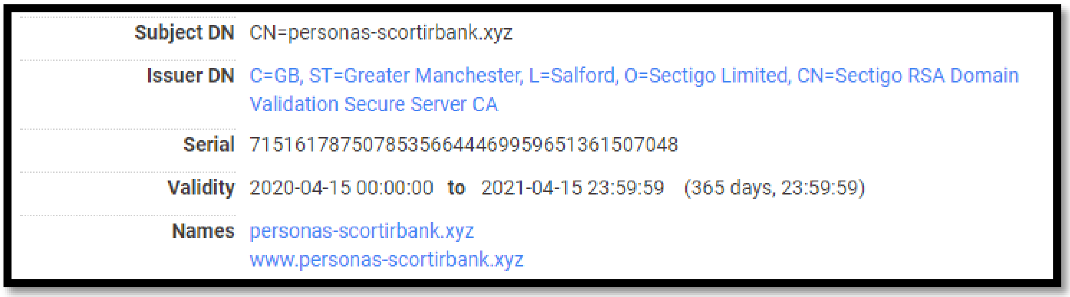


Domain pre-covid.info

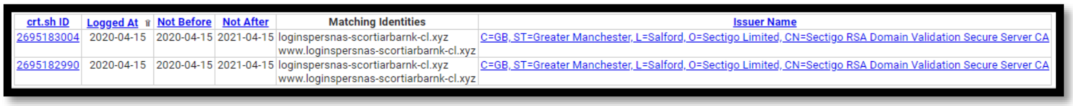
pre-covid / info / Subdomains

record type	TTL	value		
A	3600	178.159.36.139		
NS	300	ns03.freenom.com	Zones on DNS server	104.155.27.112
NS	300	ns01.freenom.com	Zones on DNS server	54.171.131.39
NS	300	ns04.freenom.com	Zones on DNS server	104.155.29.241
NS	300	ns02.freenom.com	Zones on DNS server	52.19.156.76
SOA	300	Mname	ns01.freenom.com	
		Rname	soa.freenom.com	
		Serial number	1586924097	
		Refresh	10800	
		Retry	3600	
		Expire	604800	
		Minimum TTL	3600	

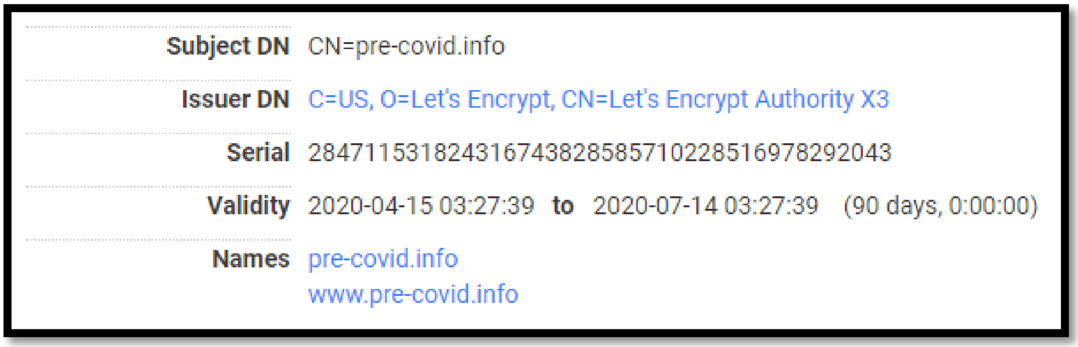
CERTIFICADOS



Subject DN	CN=personas-scortirbank.xyz
Issuer DN	C=GB, ST=Greater Manchester, L=Salford, O=Sectigo Limited, CN=Sectigo RSA Domain Validation Secure Server CA
Serial	71516178750785356644469959651361507048
Validity	2020-04-15 00:00:00 **to** 2021-04-15 23:59:59 (365 days, 23:59:59)
Names	personas-scortirbank.xyz www.personas-scortirbank.xyz

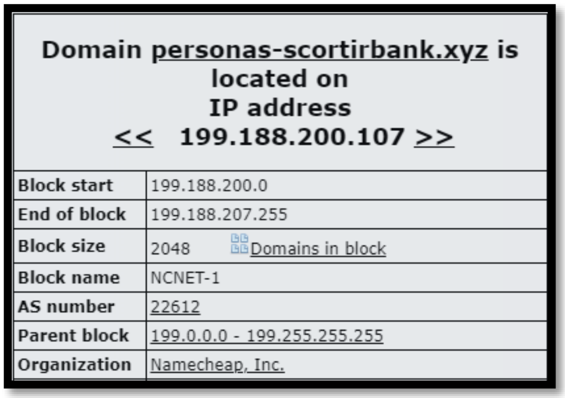


crt.sh ID	Logged At ⇧	Not Before	Not After	Matching Identities	Issuer Name
2695183004	2020-04-15	2020-04-15	2021-04-15	loginspersnas-scortiarbarnk-cl.xyz www.loginspersnas-scortiarbarnk-cl.xyz	C=GB, ST=Greater Manchester, L=Salford, O=Sectigo Limited, CN=Sectigo RSA Domain Validation Secure Server CA
2695182990	2020-04-15	2020-04-15	2021-04-15	loginspersnas-scortiarbarnk-cl.xyz www.loginspersnas-scortiarbarnk-cl.xyz	C=GB, ST=Greater Manchester, L=Salford, O=Sectigo Limited, CN=Sectigo RSA Domain Validation Secure Server CA



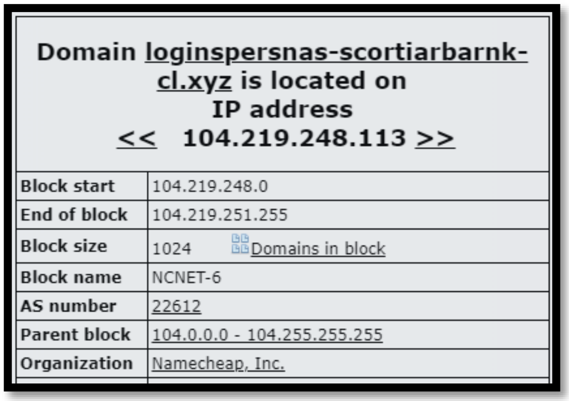
Subject DN	CN=pre-covid.info
Issuer DN	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
Serial	284711531824316743828585710228516978292043
Validity	2020-04-15 03:27:39 **to** 2020-07-14 03:27:39 (90 days, 0:00:00)
Names	pre-covid.info www.pre-covid.info

IP DE ORIGEN DONDE SE ALOJA SITIO



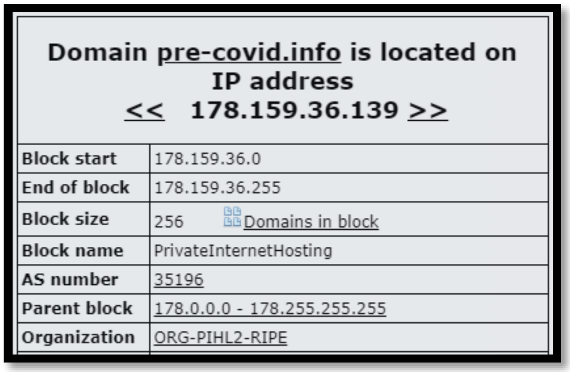
Domain personas-scortirbank.xyz is located on IP address << 199.188.200.107 >>

Block start	199.188.200.0
End of block	199.188.207.255
Block size	2048 Domains in block
Block name	NCNET-1
AS number	22612
Parent block	199.0.0.0 - 199.255.255.255
Organization	Namecheap, Inc.



Domain loginspersnas-scortiarbarnk-cl.xyz is located on IP address
<< 104.219.248.113 >>

Block start	104.219.248.0
End of block	104.219.251.255
Block size	1024 Domains in block
Block name	NCNET-6
AS number	22612
Parent block	104.0.0.0 - 104.255.255.255
Organization	Namecheap, Inc.

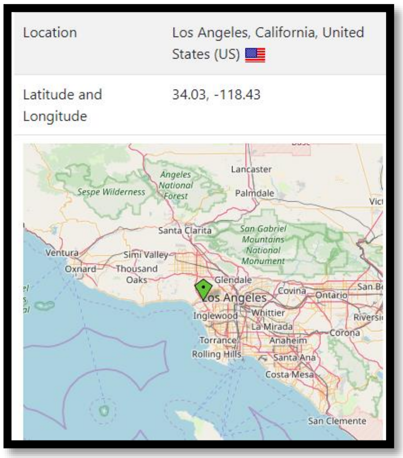


Domain pre-covid.info is located on IP address
<< 178.159.36.139 >>

Block start	178.159.36.0
End of block	178.159.36.255
Block size	256 Domains in block
Block name	PrivateInternetHosting
AS number	35196
Parent block	178.0.0.0 - 178.255.255.255
Organization	ORG-PIHL2-RIPE

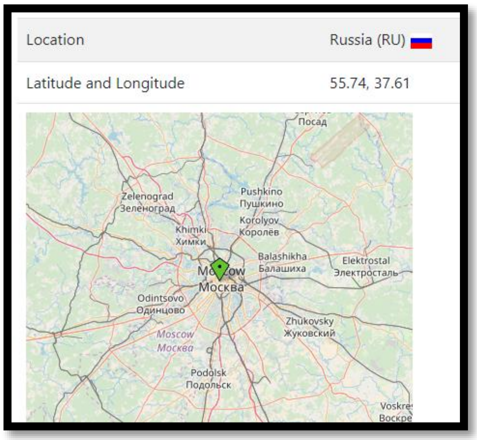
LOCALIZACIÓN

Los Angeles, california, Estados Unidos



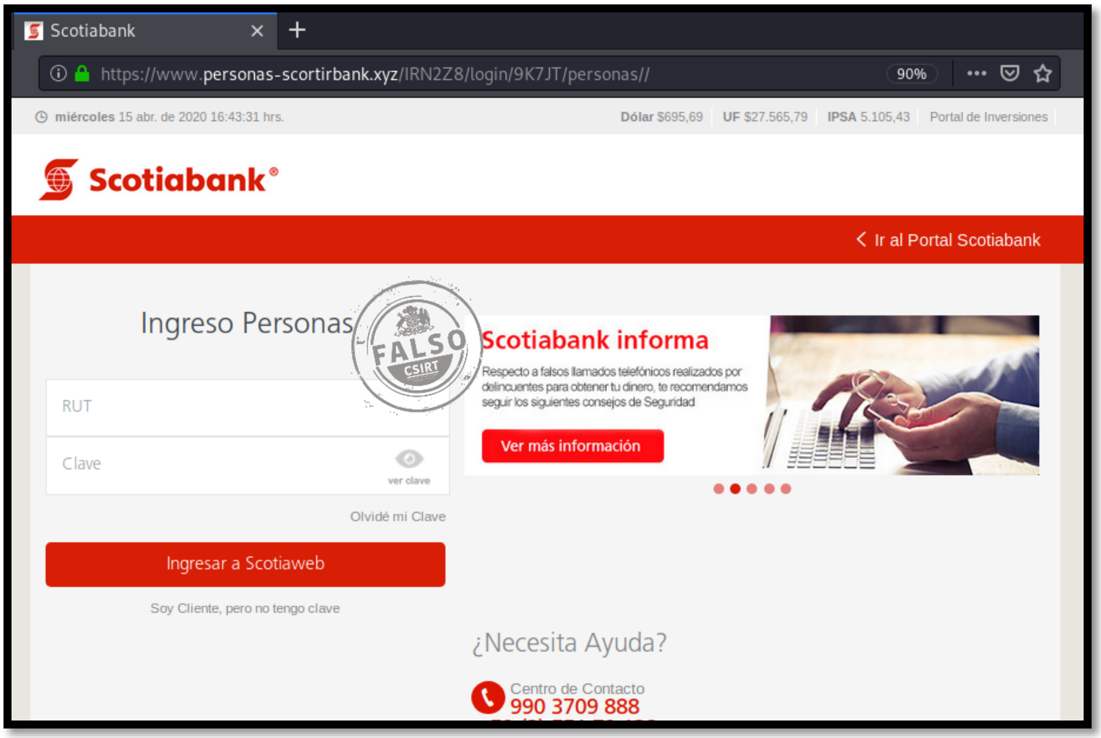
Location	Los Angeles, California, United States (US)
Latitude and Longitude	34.03, -118.43

Moscú, Federación Rusa



Location	Russia (RU)
Latitude and Longitude	55.74, 37.61

IMAGEN DEL SITIO



Scotiabank

https://www.personas-scortirbank.xyz/IRN2Z8/login/9K7JT/personas//

miércoles 15 abr. de 2020 16:43:31 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

FALSO CSIRT

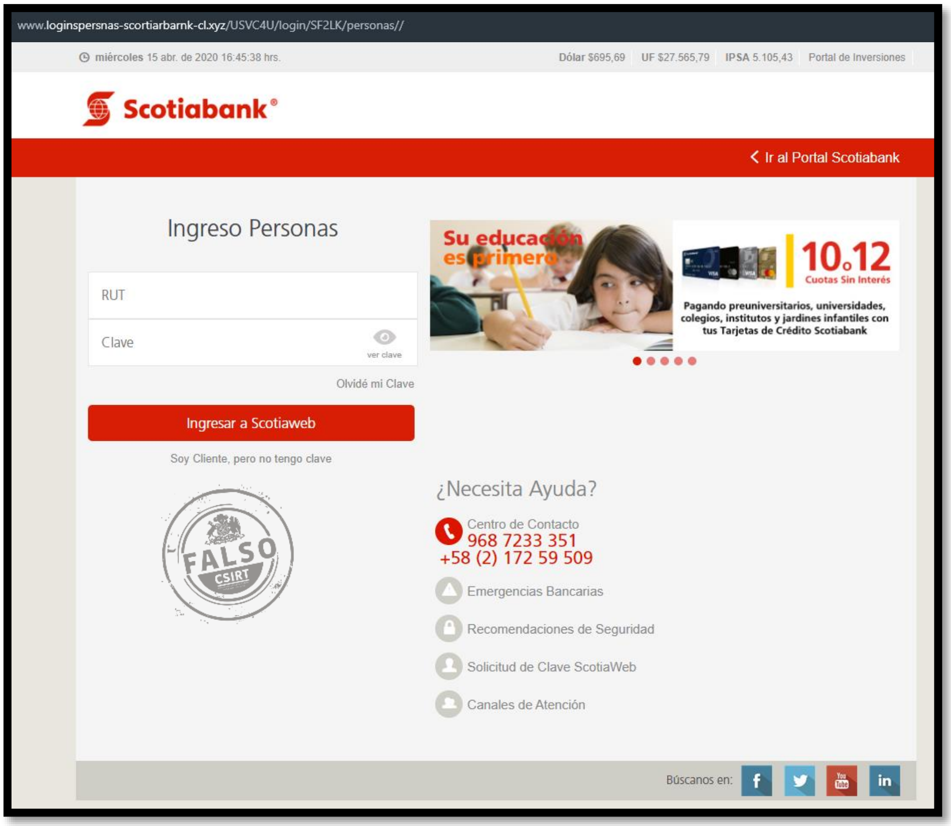
Scotiabank informa

Respecto a falsos llamados telefónicos realizados por delincuentes para obtener tu dinero, te recomendamos seguir los siguientes consejos de Seguridad

Ver más información

¿Necesita Ayuda?

Centro de Contacto
990 3709 888



www.loginspersnas-scortiarbarnk-cl.xyz/USVC4U/login/SF2LK/personas//

miércoles 15 abr. de 2020 16:45:38 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

FALSO CSIRT

Su educación es primero

10.12 Cuotas Sin Interés

Pagando preuniversitarios, universidades, colegios, institutos y jardines infantiles con tus Tarjetas de Crédito Scotiabank

¿Necesita Ayuda?

Centro de Contacto
968 7233 351
+58 (2) 172 59 509

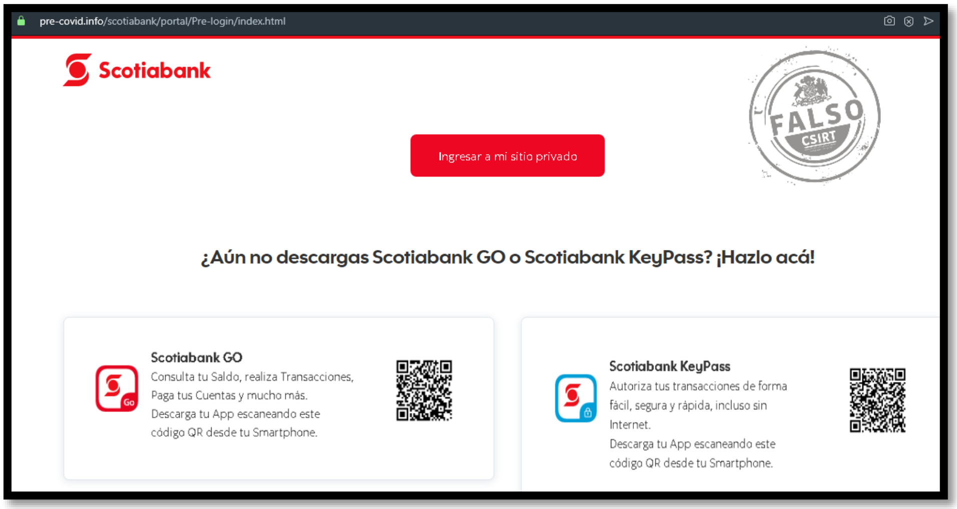
Emergencias Bancarias

Recomendaciones de Seguridad

Solicitud de Clave ScotiaWeb

Canales de Atención

Búscanos en:



pre-covid.info/scotiabank/portal/Pre-login/index.html

Scotiabank

Ingresar a mi sitio privado

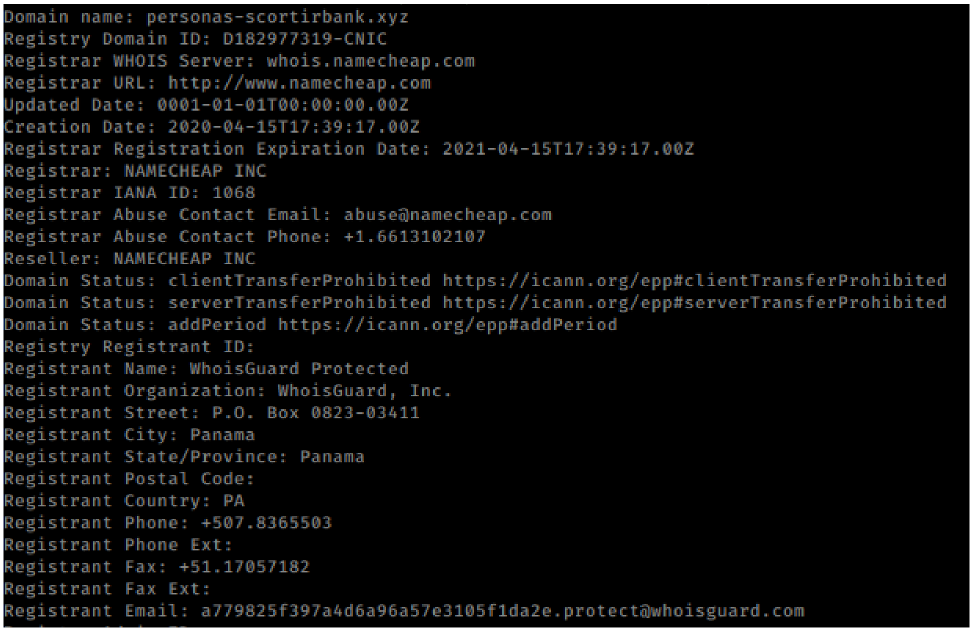
FALSO CSIRT

¿Aún no descargas Scotiabank GO o Scotiabank KeyPass? ¡Hazlo acá!

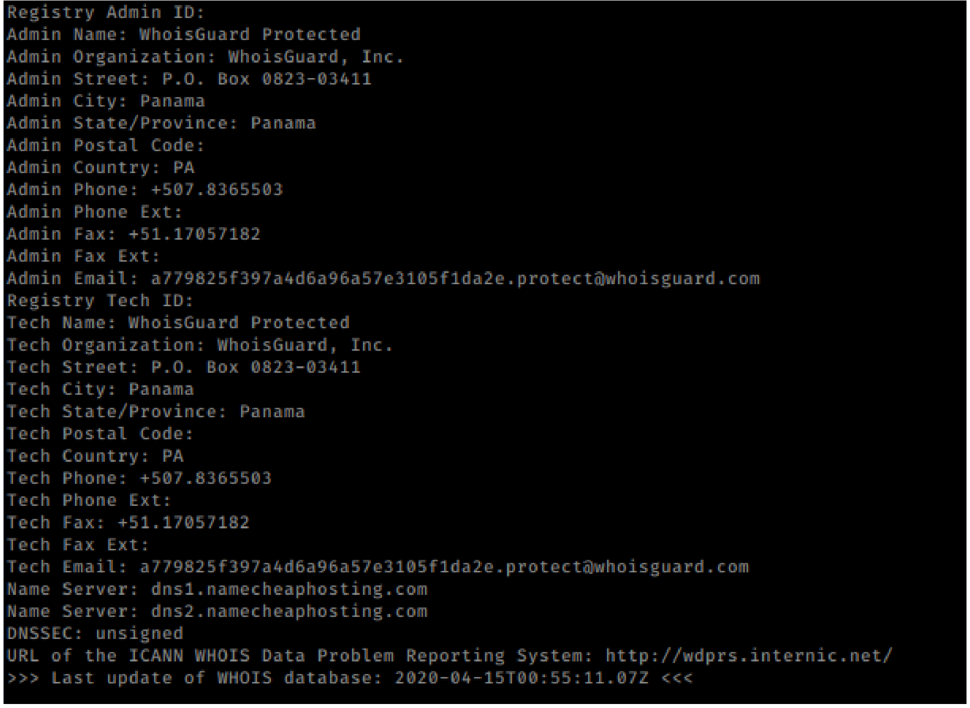
Scotiabank GO
Consulta tu Saldo, realiza Transacciones, Paga tus Cuentas y mucho más.
Descarga tu App escaneando este código QR desde tu Smartphone.

Scotiabank KeyPass
Autoriza tus transacciones de forma fácil, segura y rápida, incluso sin Internet.
Descarga tu App escaneando este código QR desde tu Smartphone.

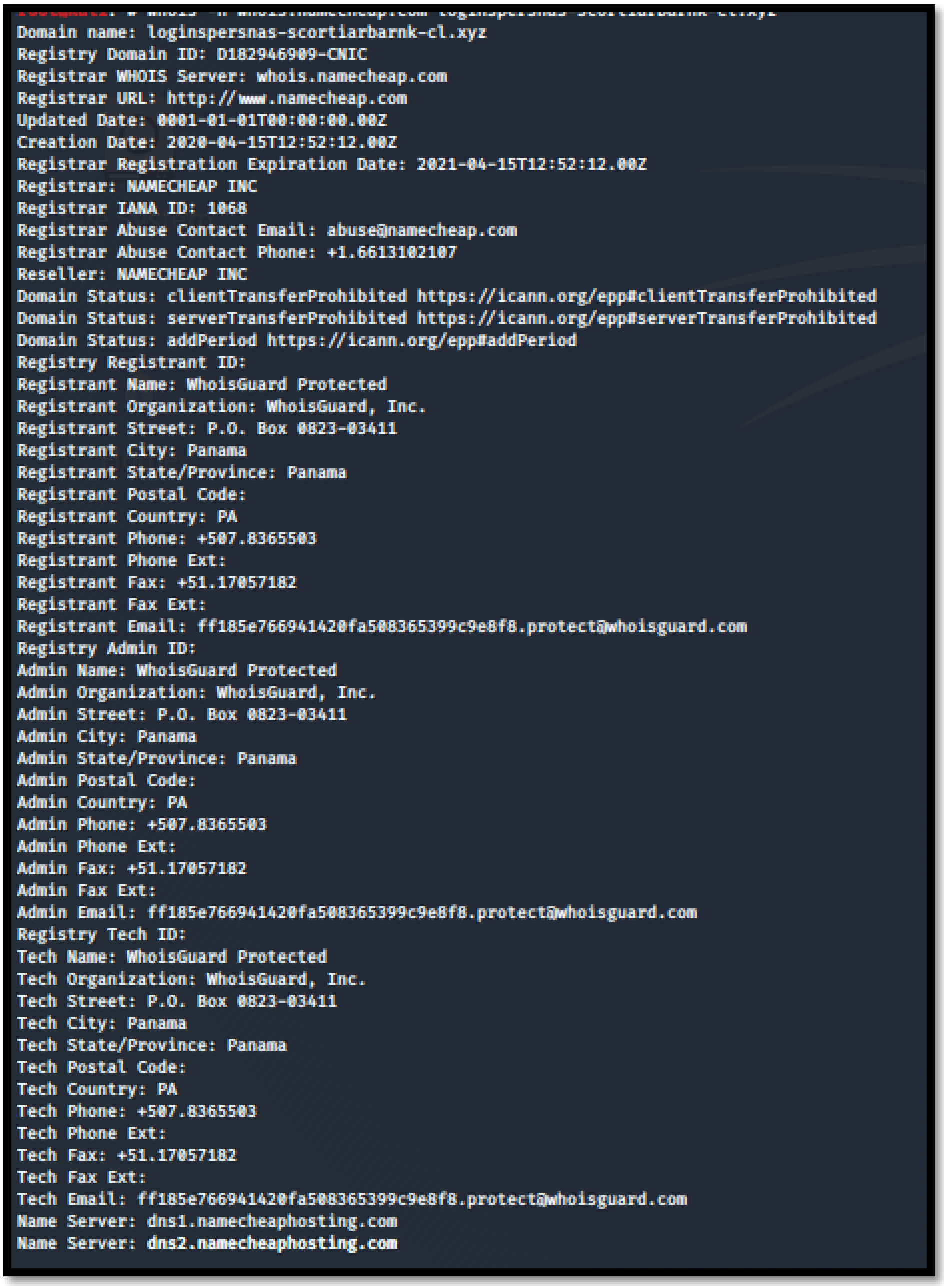
WHOIS



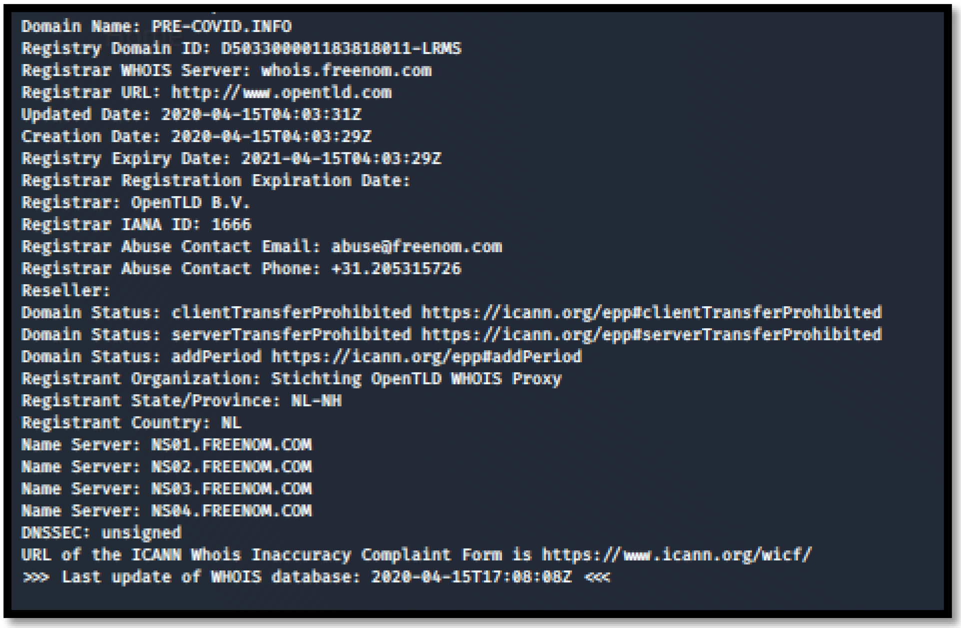
```
Domain name: personas-scortirbank.xyz
Registry Domain ID: D182977319-CNIC
Registrar WHOIS Server: whois.namecheap.com
Registrar URL: http://www.namecheap.com
Updated Date: 0001-01-01T00:00:00.00Z
Creation Date: 2020-04-15T17:39:17.00Z
Registrar Registration Expiration Date: 2021-04-15T17:39:17.00Z
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
Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
Domain Status: addPeriod https://icann.org/epp#addPeriod
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: a779825f397a4d6a96a57e3105f1da2e.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: a779825f397a4d6a96a57e3105f1da2e.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: a779825f397a4d6a96a57e3105f1da2e.protect@whoisguard.com
Name Server: dns1.namecheaphosting.com
Name Server: dns2.namecheaphosting.com
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2020-04-15T00:55:11.07Z <<<
```



```
root@kali:~# whois -h whois.namecheap.com loginspersnas-scortiarbarnk-cl.xyz
Domain name: loginspersnas-scortiarbarnk-cl.xyz
Registry Domain ID: D182946909-CNIC
Registrar WHOIS Server: whois.namecheap.com
Registrar URL: http://www.namecheap.com
Updated Date: 0001-01-01T00:00:00.00Z
Creation Date: 2020-04-15T12:52:12.00Z
Registrar Registration Expiration Date: 2021-04-15T12:52:12.00Z
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
Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
Domain Status: addPeriod https://icann.org/epp#addPeriod
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: ff185e766941420fa508365399c9e8f8.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: ff185e766941420fa508365399c9e8f8.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: ff185e766941420fa508365399c9e8f8.protect@whoisguard.com
Name Server: dns1.namecheaphosting.com
Name Server: dns2.namecheaphosting.com
```



```
Domain Name: PRE-COVID.INFO
Registry Domain ID: D503300001183818011-LRMS
Registrar WHOIS Server: whois.freenom.com
Registrar URL: http://www.opentld.com
Updated Date: 2020-04-15T04:03:31Z
Creation Date: 2020-04-15T04:03:29Z
Registry Expiry Date: 2021-04-15T04:03:29Z
Registrar Registration Expiration Date:
Registrar: OpenTLD B.V.
Registrar IANA ID: 1666
Registrar Abuse Contact Email: abuse@freenom.com
Registrar Abuse Contact Phone: +31.205315726
Reseller:
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
Domain Status: addPeriod https://icann.org/epp#addPeriod
Registrant Organization: Stichting OpenTLD WHOIS Proxy
Registrant State/Province: NL-NH
Registrant Country: NL
Name Server: NS01.FREENOM.COM
Name Server: NS02.FREENOM.COM
Name Server: NS03.FREENOM.COM
Name Server: NS04.FREENOM.COM
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form is https://www.icann.org/wicf/
>>> Last update of WHOIS database: 2020-04-15T17:08:08Z <<<
```

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: 2020.04.16 10:39:27 -04'00'