Alerta de seguridad informática	8FFR20-00267-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	17 de Marzo de 2020
Última revisión	17 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 tres 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[.]cl-login[.]club

acceso[.]scotianbak[.]club

scotia[.]cl-login[.]top

Domain cl-login.club

cl-login / club / Subdomains

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

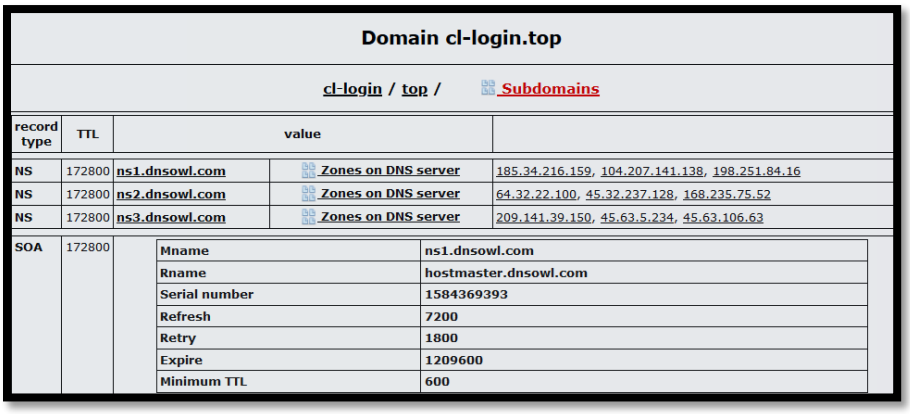
SOA	172800	Mname	ns1.dnsowl.com
		Rname	hostmaster.dnsowl.com
		Serial number	1584364002
		Refresh	7200
		Retry	1800
		Expire	1209600
		Minimum TTL	600

Domain scotianbak.club

scotianbak / club / Subdomains

record type	TTL	value		
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	64.32.22.100, 45.32.237.128, 168.235.75.52
NS	172800	ns3.dnsowl.com	Zones on DNS server	45.63.106.63, 209.141.39.150, 45.63.5.234

SOA	172800	Mname	ns1.dnsowl.com
		Rname	hostmaster.dnsowl.com
		Serial number	1584365794
		Refresh	7200
		Retry	1800
		Expire	1209600
		Minimum TTL	600



Domain cl-login.top

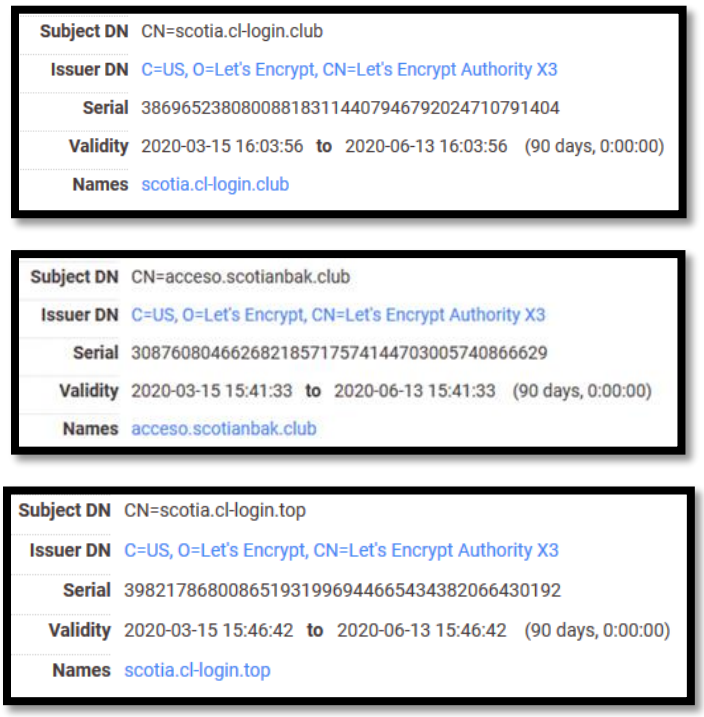
cl-login / top / Subdomains

record type	TTL	value		
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	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	1584369393
		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.cl-login.club
Issuer DN C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
Serial 386965238080088183114407946792024710791404
Validity 2020-03-15 16:03:56 **to** 2020-06-13 16:03:56 (90 days, 0:00:00)
Names scotia.cl-login.club

Subject DN CN=acceso.scotianbak.club
Issuer DN C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
Serial 308760804662682185717574144703005740866629
Validity 2020-03-15 15:41:33 **to** 2020-06-13 15:41:33 (90 days, 0:00:00)
Names acceso.scotianbak.club

Subject DN CN=scotia.cl-login.top
Issuer DN C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
Serial 398217868008651931996944665434382066430192
Validity 2020-03-15 15:46:42 **to** 2020-06-13 15:46:42 (90 days, 0:00:00)
Names scotia.cl-login.top

Ilustración 1 Certificado Utilizado en Url del sitio Falso del Banco Scotiabank

IP

139[.]59[.]94[.]0
64[.]227[.]73[.]193
68[.]183[.]42[.]216

Domain scotia.cl-login.club is located on IP address << 139.59.94.0 >>

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 acceso.scotianbak.club is located on IP address << 64.227.73.193 >>

Block start	64.224.0.0
End of block	64.227.255.255
Block size	262144 Domains in block
Block name	64-224-0-0-NET
AS number	14061
Parent block	64.0.0.0 - 64.255.255.255
Organization	Peer 1 Dedicated Hosting

Domain scotia.cl-login.top is located on IP address << 68.183.42.216 >>

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

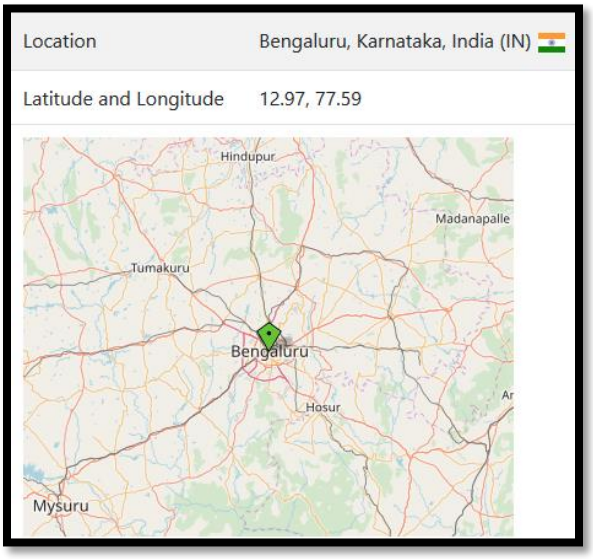
Ilustración 1 Ip de Origen donde se aloja Sitio Falso del Banco Scotiabank

Localización

Bengaluru, Karnataka, India

New York City, New York, Estados Unidos

Londres, Reino Unido



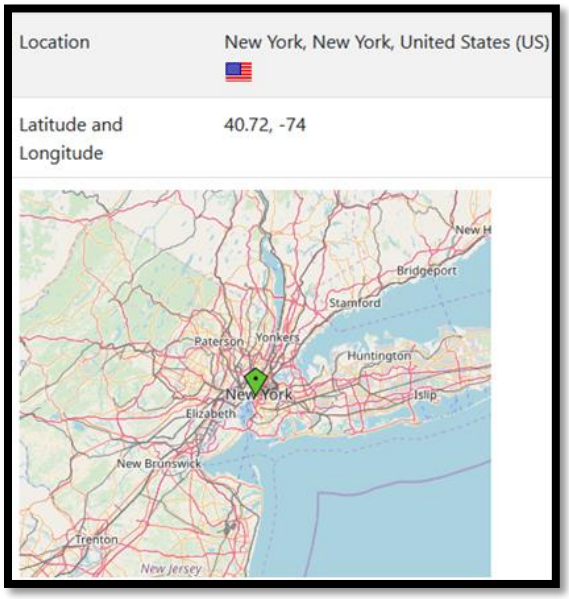
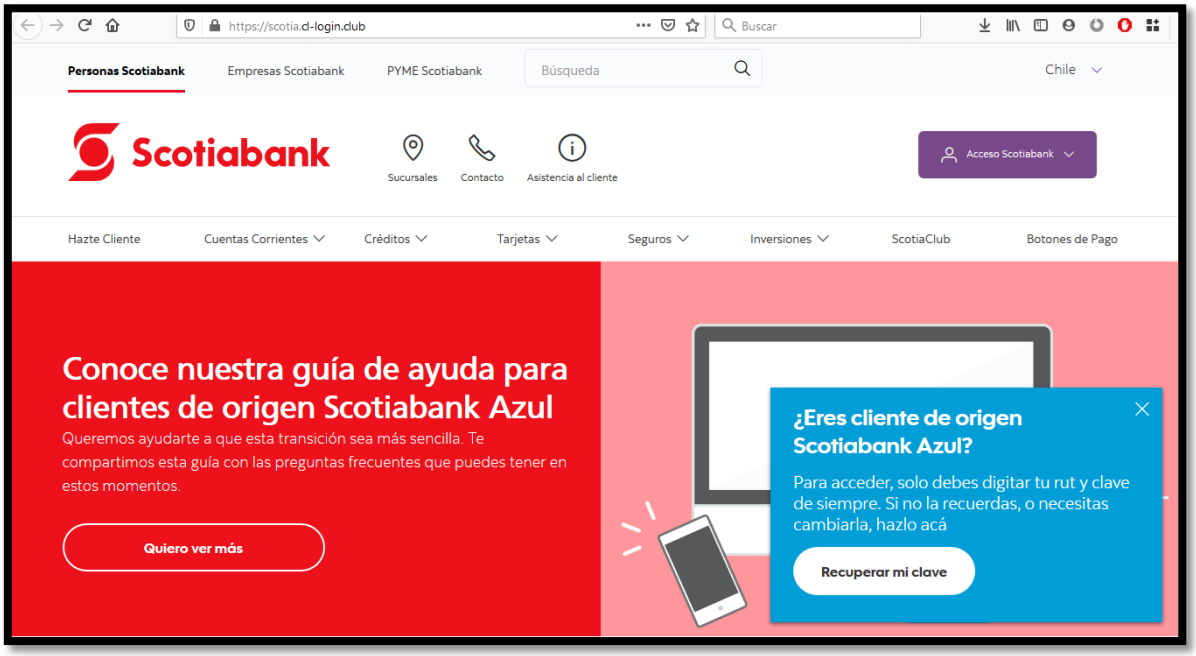
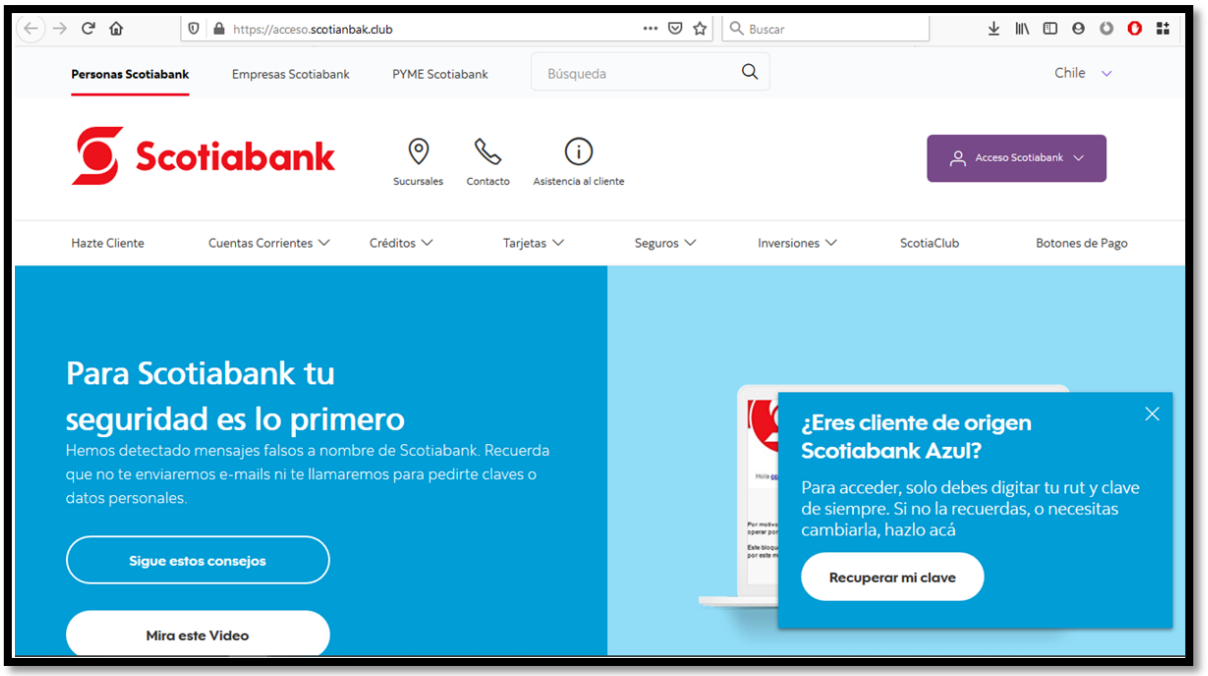
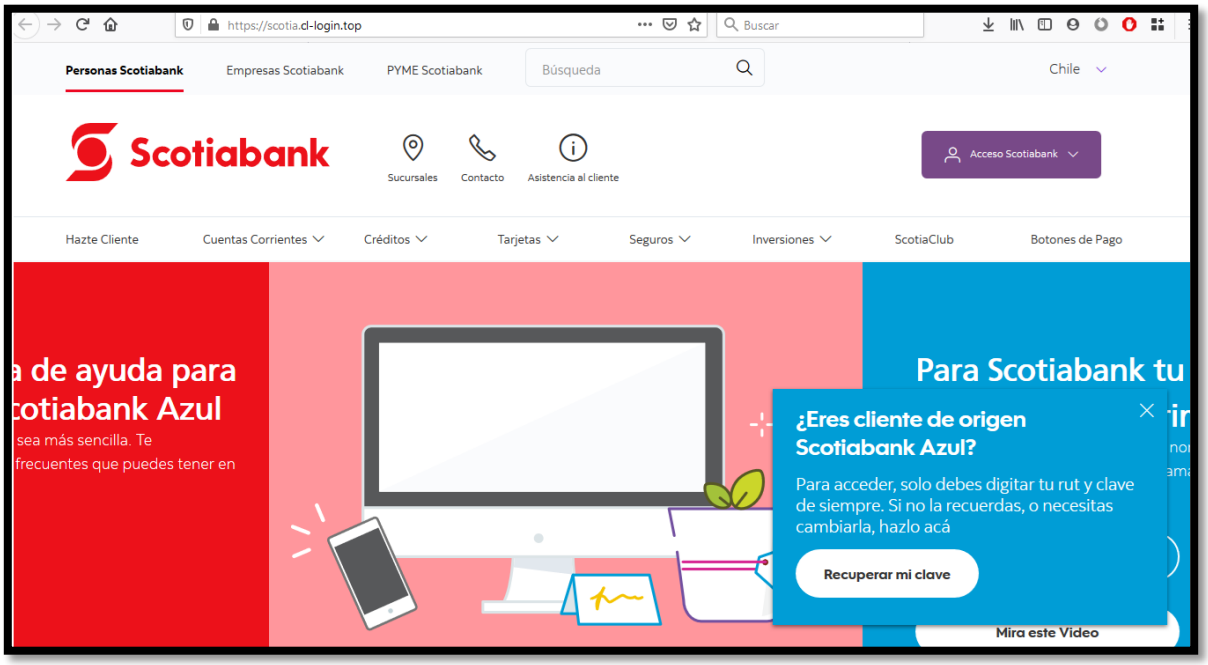


Imagen del sitio




https://acceso.scotianbak.club
Buscar
Personas Scotiabank
Empresas Scotiabank
PYME Scotiabank
Búsqueda
Chile
Scotiabank
Sucursales
Contacto
Asistencia al cliente
Acceso Scotiabank
Hazte Cliente
Cuentas Corrientes
Créditos
Tarjetas
Seguros
Inversiones
ScotiaClub
Botones de Pago
Para Scotiabank tu seguridad es lo primero
Hemos detectado mensajes falsos a nombre de Scotiabank. Recuerda que no te enviaremos e-mails ni te llamaremos para pedirte claves o datos personales.
Sigue estos consejos
Mira este Video
¿Eres cliente de origen Scotiabank Azul?
Para acceder, solo debes digitar tu rut y clave de siempre. Si no la recuerdas, o necesitas cambiarla, hazlo acá
Recuperar mi clave


https://scotia.cl-login.top
Buscar
Personas Scotiabank
Empresas Scotiabank
PYME Scotiabank
Búsqueda
Chile
Scotiabank
Sucursales
Contacto
Asistencia al cliente
Acceso Scotiabank
Hazte Cliente
Cuentas Corrientes
Créditos
Tarjetas
Seguros
Inversiones
ScotiaClub
Botones de Pago
Para Scotiabank tu
¿Eres cliente de origen Scotiabank Azul?
Para acceder, solo debes digitar tu rut y clave de siempre. Si no la recuerdas, o necesitas cambiarla, hazlo acá
Recuperar mi clave
Mira este Video

Whois

```
Domain Name: cl-login.club
Registry Domain ID: DF9AEF59D32904E718435B4B0491A5BA6-NSR
Registrar WHOIS Server: whois.namesilo.com
Registrar URL: https://www.namesilo.com/
Updated Date: 2020-03-15T07:00:00Z
Creation Date: 2020-03-15T07:00:00Z
Registrar Registration Expiration Date: 2021-03-15T07:00:00Z
Registrar: NameSilo, LLC
Registrar IANA ID: 1479
Registrar Abuse Contact Email: abuse@namesilo.com
Registrar Abuse Contact Phone: +1.4805240066
Domain Status: clientTransferProhibited https://www.icann.org/epp#clientTransferProhibited
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-053eb07e0d28d6fc42f9a95a1c2bf5ee@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-053eb07e0d28d6fc42f9a95a1c2bf5ee@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-053eb07e0d28d6fc42f9a95a1c2bf5ee@privacyguardian.org
Name Server: NS1.DNSOWL.COM
Name Server: NS2.DNSOWL.COM
Name Server: NS3.DNSOWL.COM
DNSSEC: unsigned
```

```
Domain Name: scotianbak.club
Registry Domain ID: D5D50438A997F4D61B81DE9EDC18981C4-NSR
Registrar WHOIS Server: whois.namesilo.com
Registrar URL: https://www.namesilo.com/
Updated Date: 2020-03-15T07:00:00Z
Creation Date: 2020-03-15T07:00:00Z
Registrar Registration Expiration Date: 2021-03-15T07:00:00Z
Registrar: NameSilo, LLC
Registrar IANA ID: 1479
Registrar Abuse Contact Email: abuse@namesilo.com
Registrar Abuse Contact Phone: +1.4805240066
Domain Status: clientTransferProhibited https://www.icann.org/epp#clientTransferProhibited
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-8045b073f6fec9e99c87f64203737641@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-8045b073f6fec9e99c87f64203737641@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-8045b073f6fec9e99c87f64203737641@privacyguardian.org
Name Server: NS1.DNSOWL.COM
Name Server: NS2.DNSOWL.COM
Name Server: NS3.DNSOWL.COM
DNSSEC: unsigned
```

```
Domain Name: cl-login.top
Registry Domain ID: 20200315g10001g-35645037
Registrar WHOIS Server: whois.namesilo.com
Registrar URL: https://www.namesilo.com/
Updated Date: 2020-03-15T07:00:00Z
Creation Date: 2020-03-15T07:00:00Z
Registrar Registration Expiration Date: 2021-03-15T07:00:00Z
Registrar: NameSilo, LLC
Registrar IANA ID: 1479
Registrar Abuse Contact Email: abuse@namesilo.com
Registrar Abuse Contact Phone: +1.4805240066
Domain Status: clientTransferProhibited https://www.icann.org/epp#clientTransferProhibited
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-d61482246fa79cfe97e4d0eda639a18a@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-d61482246fa79cfe97e4d0eda639a18a@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-d61482246fa79cfe97e4d0eda639a18a@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.