Alerta de seguridad informática	8FFR-00121-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	23 de Noviembre de 2019
Última revisión	23 de Noviembre de 2019

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 3 portales bancarios fraudulentos asociados a 3 IPs que suplantan el sitio web oficial de **Banco Estado**, lo 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

URL Sitio Clonado:
http[://]hotelconnected[.]com/www[.]bancoestado[.]cl/imagenes/comun2008/banca-en-linea-personas[.]html

www[.]gsmshopnoord[.]nl/wp-content/www[.]bancoestado[.]cl/imagenes/comun2008/banca-en-linea-personas[.]html

https[://]www[.]barcoestadocl[.]xyz/imagenes/comun2009/en-linea-personas[.]php

Domain hotelconnected.com

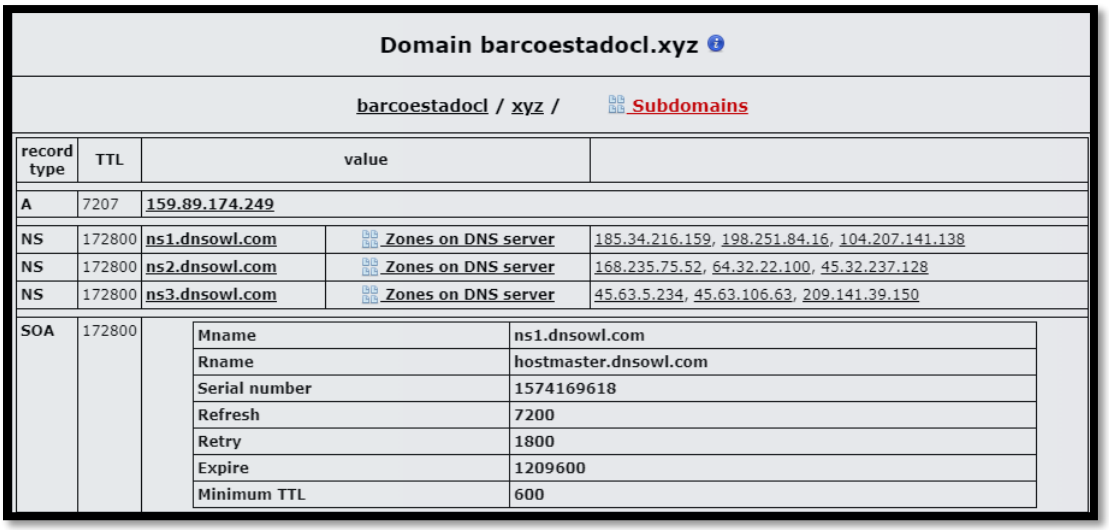
hotelconnected / com / Subdomains

record type	TTL	value		
A	600	194.147.120.213		
NS	600	ns2.galaxywebsolutions.com	Zones on DNS server	82.163.78.110
NS	600	ns1.galaxywebsolutions.com	Zones on DNS server	194.147.120.199
MX	600	0 hotelconnected.com		
TXT	600	v=spf1 ip4:194.147.120.204 ip4:194.147.120.213 ip4:193.111.184.204 +ip4:193.111.184.213 +a +mx ~all		
SOA	600	Mname: ns1.galaxywebsolutions.com Rname: info.galaxywebsolutions.com Serial number: 2019110700 Refresh: 3600 Retry: 7200 Expire: 1209600 Minimum TTL: 86400		

Domain gsmshopnoord.nl

gsmshopnoord / nl / Subdomains

record type	TTL	value		
A	10800	160.153.129.229		
NS	3600	ns58.domaincontrol.com	Zones on DNS server	173.201.76.29
NS	3600	ns57.domaincontrol.com	Zones on DNS server	97.74.108.29
MX	3600	10 mx.zoho.com		136.143.190.121
MX	3600	20 mx2.zoho.com		204.141.32.121
MX	3600	50 mx3.zoho.com		136.143.190.121
TXT	600	v=spf1 include:zoho.com ~all		
TXT	600	facebook-domain-verification=rcr4c6wcvnbxd66dtriuvl74hfq7dc		
SOA	3600	Mname: ns57.domaincontrol.com Rname: dns.jomax.net Serial number: 2019111000 Refresh: 28800 Retry: 7200 Expire: 604800 Minimum TTL: 600		



Domain barcoestadocl.xyz

barcoestadocl / xyz / Subdomains

record type	TTL	value		
A	7207	159.89.174.249		
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	168.235.75.52, 64.32.22.100, 45.32.237.128
NS	172800	ns3.dnsowl.com	Zones on DNS server	45.63.5.234, 45.63.106.63, 209.141.39.150
SOA	172800			

Mname	ns1.dnsowl.com
Rname	hostmaster.dnsowl.com
Serial number	1574169618
Refresh	7200
Retry	1800
Expire	1209600
Minimum TTL	600

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

Certificados

Criteria	Identity = 'hotelconnected.com'

Certificates

crt.sh ID	Logged At ⇧	Not Before	Not After	Issuer Name
2023469707	2019-10-21	2019-10-20	2020-01-18	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
2018950782	2019-10-21	2019-10-20	2020-01-18	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1809399953	2019-08-21	2019-08-20	2019-11-18	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1791904706	2019-08-21	2019-08-20	2019-11-18	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1620513761	2019-06-21	2019-06-20	2019-09-18	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1597782923	2019-06-21	2019-06-20	2019-09-18	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1405077201	2019-04-21	2019-04-20	2019-07-19	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1405075874	2019-04-21	2019-04-20	2019-07-19	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1212301328	2019-02-18	2019-02-18	2019-05-19	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1212302183	2019-02-18	2019-02-18	2019-05-19	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1040609948	2018-12-19	2018-12-19	2019-03-19	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1040607581	2018-12-19	2018-12-19	2019-03-19	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
873760599	2018-10-19	2018-10-18	2019-01-16	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
873761407	2018-10-19	2018-10-18	2019-01-16	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
747601932	2018-08-19	2018-08-18	2018-11-16	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
670183015	2018-08-19	2018-08-18	2018-11-16	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
542946152	2018-06-19	2018-06-18	2018-09-16	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
536063349	2018-06-19	2018-06-18	2018-09-16	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
412760890	2018-04-19	2018-04-18	2018-07-17	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
404999649	2018-04-19	2018-04-18	2018-07-17	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3

Criteria	Identity = 'www.barcoestadocl.xyz'

Certificates

crt.sh ID	Logged At ⇧	Not Before	Not After	Issuer Name
2127231955	2019-11-18	2019-11-18	2020-02-16	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
2127232015	2019-11-18	2019-11-18	2020-02-16	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3

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

IP

194.147.120.213

160.153.129.229

159.89.174.249

Domain hotelconnected.com is located on IP address << 194.147.120.213 >>	
Block start	194.147.120.192
End of block	194.147.120.255
Block size	64 Domains in block
Block name	GalaxyWebSolutions
AS number	59816
Parent block	194.147.120.0 - 194.147.123.255
Organization	
City	Cheltenham
Region/State	England
Country	GB , United Kingdom
Host name	vortex.galaxywebsolutions.com
Domains	1 hotelconnected.com

Domain gsmshopnoord.nl is located on IP address << 160.153.129.229 >>	
Block start	160.153.0.0
End of block	160.153.255.255
Block size	65536 Domains in block
Block name	GO-DADDY-COM-LLC
AS number	26496
Parent block	160.0.0.0 - 160.255.255.255
Organization	GoDaddy.com, LLC
City	Scottsdale
Region/State	Arizona
Country	US , United States
Reg. date	2011-09-01
Host name	ip-160-153-129-229.ip.secureserver.net
Web server	Apache/2.4.23

Domain barcoestadocl.xyz is located on IP address << 159.89.174.249 >>

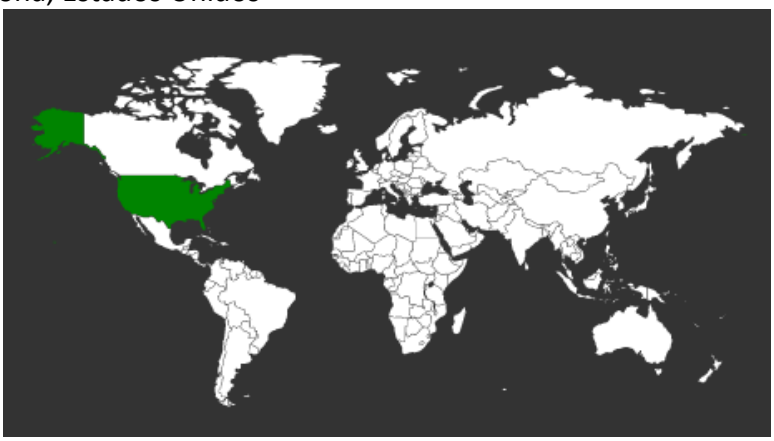
Block start	159.89.0.0
End of block	159.89.255.255
Block size	65536 Domains in block
Block name	FCCL
AS number	14061
Parent block	159.0.0.0 - 159.255.255.255
Organization	FletcherChallengeCanadaLimited
City	Vancouver
Region/State	
Country	CA , Canada
Reg. date	1992-03-30
Host name	no record in reverse zone
Domains	1 barcoestadocl.xyz

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

Localización

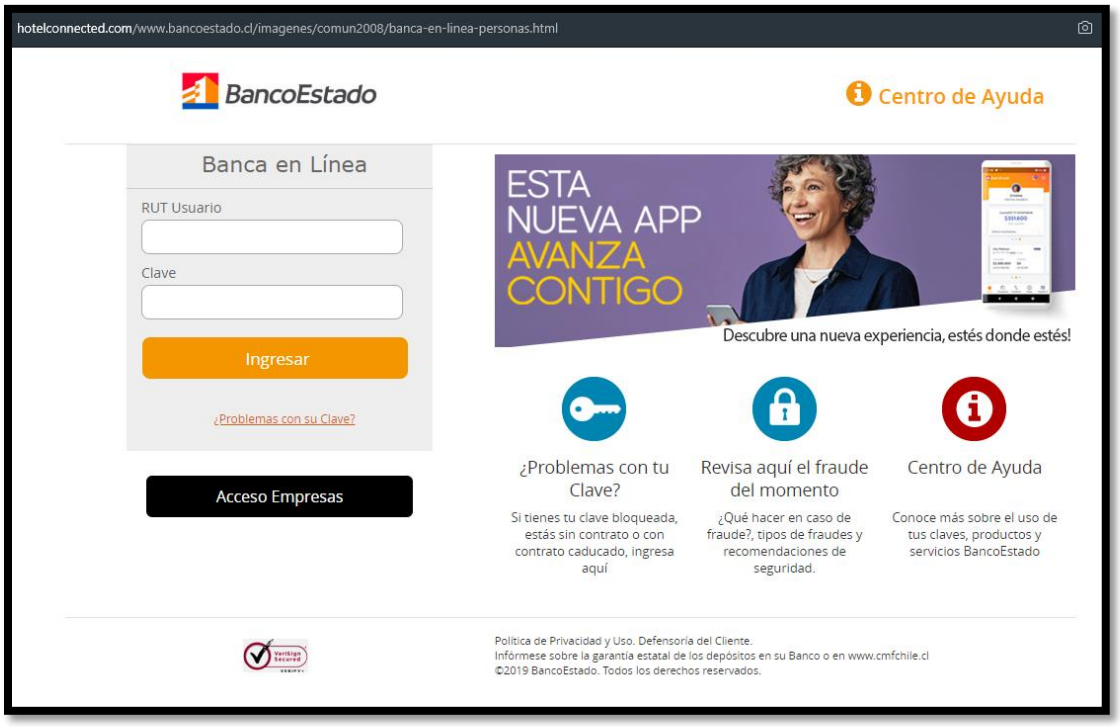
Cheltenham, Reino Unido

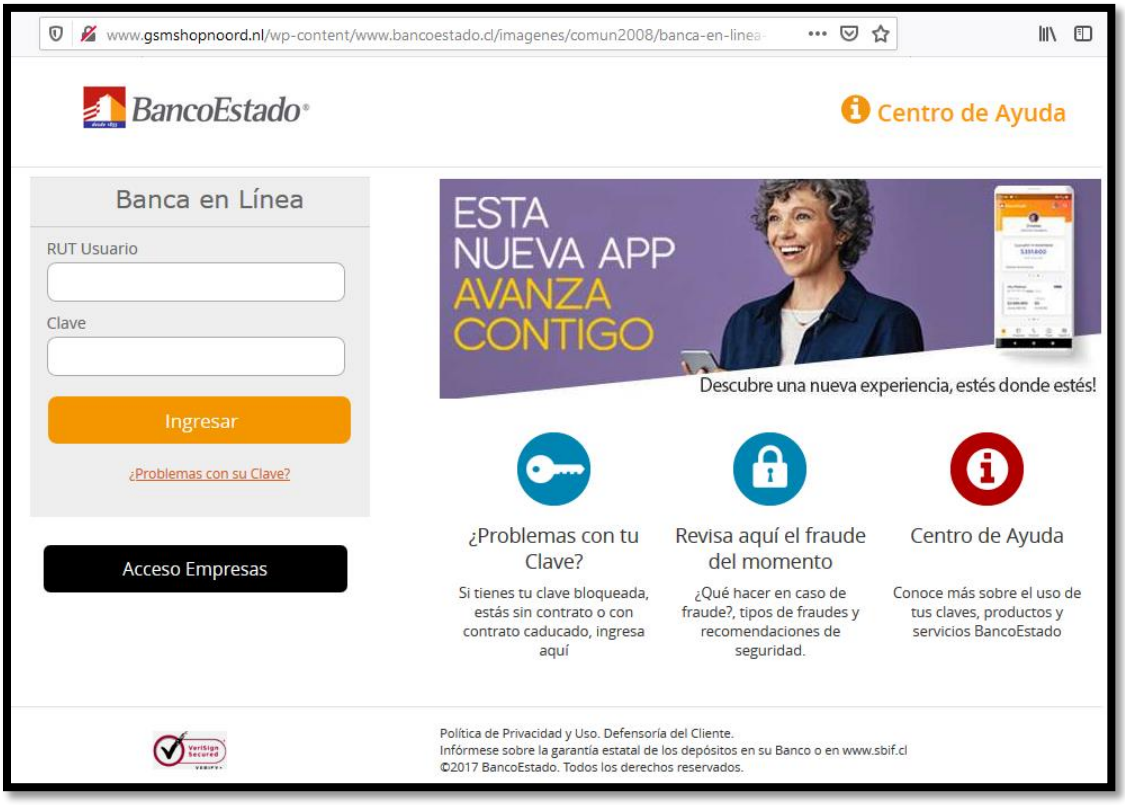
Scottsdale, Arizona, Estados Unidos

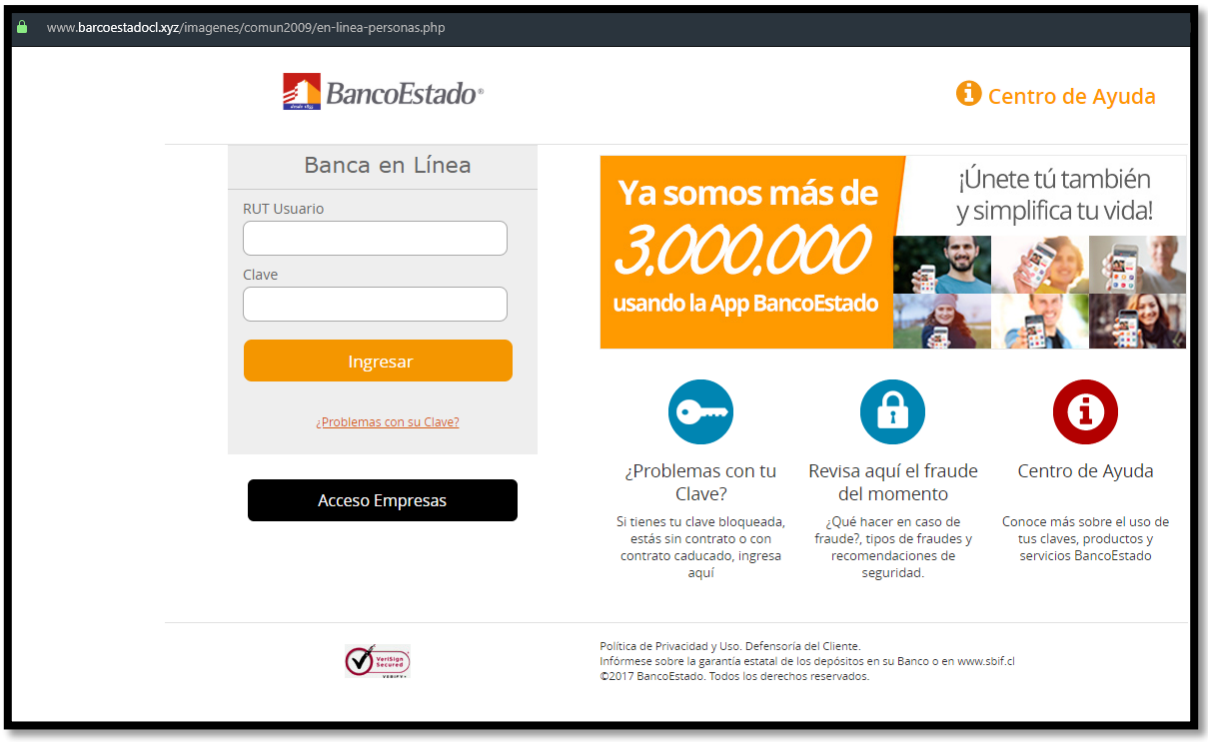


Bangalore, Karnataka, India

Imagen del sitio






www.barcoestadocl.xyz/imagenes/comun2009/en-linea-personas.php
BancoEstado
Centro de Ayuda
Banca en Línea
RUT Usuario
Clave
Ingresar
¿Problemas con su Clave?
Acceso Empresas
Ya somos más de
3.000.000
usando la App BancoEstado
¡Únete tú también
y simplifica tu vida!
¿Problemas con tu Clave?
Si tienes tu clave bloqueada, estás sin contrato o con contrato caducado, ingresa aquí
Revisa aquí el fraude del momento
¿Qué hacer en caso de fraude?, tipos de fraudes y recomendaciones de seguridad.
Centro de Ayuda
Conoce más sobre el uso de tus claves, productos y servicios BancoEstado
Política de Privacidad y Uso. Defensoría del Cliente.
Infórmese sobre la garantía estatal de los depósitos en su Banco o en www.sbif.cl
©2017 BancoEstado. Todos los derechos reservados.

Whois

```
Domain Name: HOTELCONNECTED.COM
Registry Domain ID: 583066610_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: http://www.godaddy.com
Updated Date: 2019-09-07T10:50:25Z
Creation Date: 2006-09-06T10:57:47Z
Registrar Registration Expiration Date: 2020-09-06T10:57:47Z
Registrar: GoDaddy.com, LLC
Registrar IANA ID: 146
Registrar Abuse Contact Email: abuse@godaddy.com
Registrar Abuse Contact Phone: +1.4806242505
Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited http://www.icann.org/epp#clientUpdateProhibited
Domain Status: clientRenewProhibited http://www.icann.org/epp#clientRenewProhibited
Domain Status: clientDeleteProhibited http://www.icann.org/epp#clientDeleteProhibited
Registrant Organization: Crewconnected
Registrant State/Province: Maghull
Registrant Country: UK
Registrant Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=HOTELCONNECTED.COM
Admin Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=HOTELCONNECTED.COM
Tech Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=HOTELCONNECTED.COM
Name Server: NS5.GALAXYWEBSOLUTIONS.COM
Name Server: NS6.GALAXYWEBSOLUTIONS.COM
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2019-11-18T16:00:00Z <<<
```

```
Domain name: gsmshopnoord.nl
Status:      active

Registrar:
   Hostnet B.V.
   De Ruijterkade 6
   1013AA Amsterdam
   Netherlands

Abuse Contact:
   +31.207500800
   abuse@hostnet.nl

DNSSEC:      no

Domain nameservers:
   ns57.domaincontrol.com
   ns58.domaincontrol.com

Record maintained by: NL Domain Registry
```

```
Domain Name: barcoestado.xyz
Registry Domain ID: D107517131-CNIC
Registrar WHOIS Server: whois.namesilo.com
Registrar URL: https://www.namesilo.com/
Updated Date: 2019-11-18T07:00:00Z
Creation Date: 2019-06-11T07:00:00Z
Registrar Registration Expiration Date: 2020-06-11T07:00:00Z
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#clientTransfer
Prohibited
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-9c13129fd807c6d5933ff705875c8055@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-9c13129fd807c6d5933ff705875c8055@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-9c13129fd807c6d5933ff705875c8055@privacyguardian.org
Name Server: NS1.DNSOWL.COM
Name Server: NS2.DNSOWL.COM
Name Server: NS3.DNSOWL.COM
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2019-11-19T07:00:00Z <<<
```

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