

Alerta de seguridad informática	8FFR20-00174-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	07 de enero de 2020
Última revisión	07 de enero 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 afectada a actualizaciones, por lo cual se recomienda establecer una cuarentena preventiva respecto de los loC 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 loC 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 siete portales fraudulentos asociados a una IP que suplantan el sitio web oficial de **Scotiabank**, los que podrían 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

login-scotia[.]cl[.]gcc-chile[.]info  
 login-scotia[.]cl[.]gcc-chile[.]info/Personas/  
 login-scotia[.]cl[.]gcc-chile[.]info/login/personas/  
 login-scotia[.]cl[.]gcc-chile[.]info/portalempresas/  
 scotia-cl[.]u0z[.]site  
 scotia-cl[.]u0z[.]site/login/personas/  
 scotia-cl[.]u0z[.]site/portalempresas/

Domain gcc-chile.info 																	
gcc-chile / info /  Subdomains																	
record type	TTL	value															
A	7207	<a href="#">139.59.17.209</a>															
NS	172800	<a href="#">ns1.dnsowl.com</a>	 <a href="#">Zones on DNS server</a> <a href="#">185.34.216.159</a> , <a href="#">198.251.84.16</a> , <a href="#">104.207.141.138</a>														
NS	172800	<a href="#">ns2.dnsowl.com</a>	 <a href="#">Zones on DNS server</a> <a href="#">168.235.75.52</a> , <a href="#">45.32.237.128</a> , <a href="#">64.32.22.100</a>														
NS	172800	<a href="#">ns3.dnsowl.com</a>	 <a href="#">Zones on DNS server</a> <a href="#">45.63.106.63</a> , <a href="#">209.141.39.150</a> , <a href="#">45.63.5.234</a>														
SOA	172800	<table border="1"> <tr> <td>Mname</td> <td>ns1.dnsowl.com</td> </tr> <tr> <td>Rname</td> <td>hostmaster.dnsowl.com</td> </tr> <tr> <td>Serial number</td> <td>1578335422</td> </tr> <tr> <td>Refresh</td> <td>7200</td> </tr> <tr> <td>Retry</td> <td>1800</td> </tr> <tr> <td>Expire</td> <td>1209600</td> </tr> <tr> <td>Minimum TTL</td> <td>600</td> </tr> </table>		Mname	ns1.dnsowl.com	Rname	hostmaster.dnsowl.com	Serial number	1578335422	Refresh	7200	Retry	1800	Expire	1209600	Minimum TTL	600
Mname	ns1.dnsowl.com																
Rname	hostmaster.dnsowl.com																
Serial number	1578335422																
Refresh	7200																
Retry	1800																
Expire	1209600																
Minimum TTL	600																

Search domain: scotia-cl.u0z.site		
Select ip address for continue		
ip	domain	updated
<a href="#">104.27.168.38</a>	scotia-cl.u0z.site	2020-01-06
<a href="#">104.27.169.38</a>	scotia-cl.u0z.site	2020-01-06

Ilustración 1 Dominio donde se Aloja Url de SCOTIABANK, Falso y DNS que utiliza

## Certificados


<b>Subject DN</b>	CN=login-scotia.cl.gcc-chile.info
<b>Issuer DN</b>	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
<b>Serial</b>	318988530362690367123892703258536891100584
<b>Validity</b>	2020-01-06 14:58:23 to 2020-04-05 14:58:23 (90 days, 0:00:00)
<b>Names</b>	login-scotia.cl.gcc-chile.info


<b>Subject DN</b>	CN=scotia-cl.u0z.site
<b>Issuer DN</b>	C=US, ST=TX, L=Houston, O=cPanel, Inc., CN=cPanel, Inc. Certification Authority
<b>Serial</b>	200589998283981465396914614582085713567
<b>Validity</b>	2020-01-05 00:00:00 to 2020-04-04 23:59:59 (90 days, 23:59:59)
<b>Names</b>	scotia-cl.u0z.site www.scotia-cl.u0z.site


Ilustración 2 Certificado Utilizado en Url del sitio Falso de SCOTIABANK

## IP

139[.]59[.]17[.]209  
104[.]27[.]168[.]38  
104[.]27[.]169[.]38

<b>Domain <a href="https://login-scotia.cl.gcc-chile.info">login-scotia.cl.gcc-chile.info</a> is located on IP address &lt;&lt; 139.59.17.209 &gt;&gt;</b>	
<b>Block start</b>	139.59.0.0
<b>End of block</b>	139.59.255.254
<b>Block size</b>	65535 <a href="#">Domains in block</a>
<b>Block name</b>	DIGITALOCEAN-AP
<b>AS number</b>	14061
<b>Parent block</b>	139.59.0.0 - 139.59.255.255
<b>Organization</b>	DigitalOcean, LLC
<b>Country</b>	 SG , Singapore
<b>Host name</b>	no record in reverse zone
<b>Domains</b>	1 <a href="https://login-scotia.cl.gcc-chile.info">login-scotia.cl.gcc-chile.info</a>

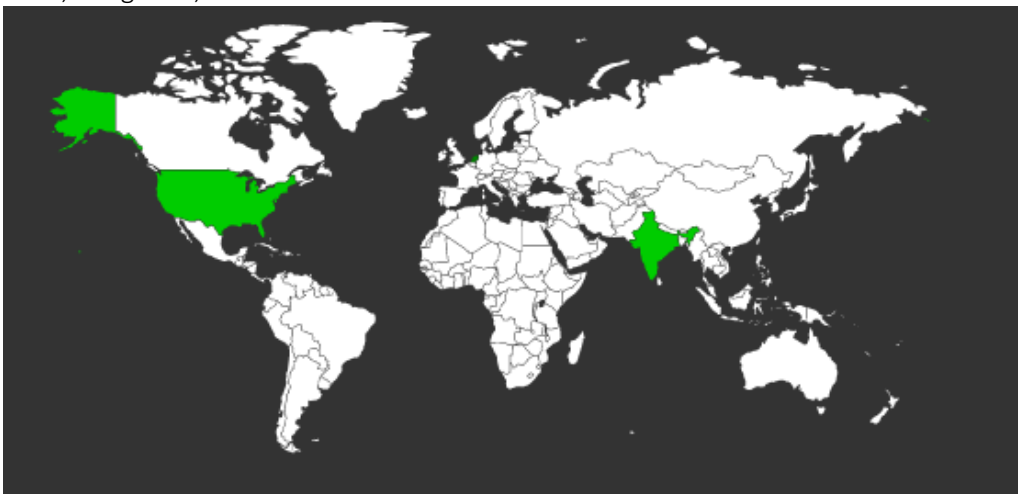
Domain <u>scotia-cl.u0z.site</u> is located on IP address << 104.27.168.38 >>	
Block start	104.16.0.0
End of block	104.31.255.255
Block size	1048576 <a href="#">Domains in block</a>
Block name	CLOUDFLARENET
AS number	13335
Parent block	104.0.0.0 - 104.255.255.255
Organization	CloudFlare, Inc.
City	San Francisco
Region/State	California
Country	 US , United States
Reg. date	2014-03-28
Host name	no record
Web server	cloudflare-nginx

Domain <u>scotia-cl.u0z.site</u> is located on IP address << 104.27.169.38 >>	
Block start	104.16.0.0
End of block	104.31.255.255
Block size	1048576 <a href="#">Domains in block</a>
Block name	CLOUDFLARENET
AS number	13335
Parent block	104.0.0.0 - 104.255.255.255
Organization	CloudFlare, Inc.
City	San Francisco
Region/State	California
Country	 US , United States
Reg. date	2014-03-28
Host name	no record
Web server	cloudflare-nginx

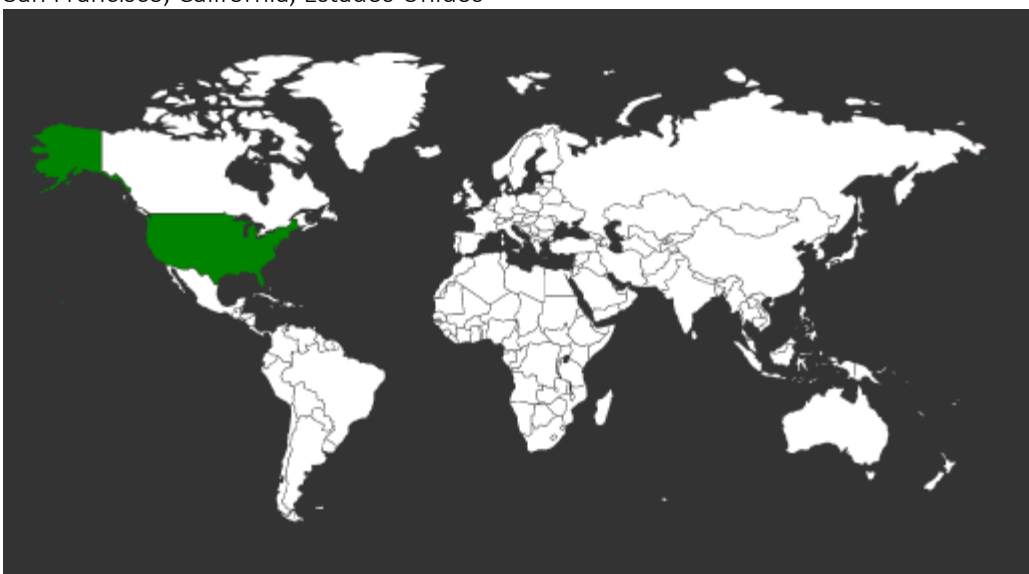
*Ilustración 3 Ip de Origen donde se aloja Sitio Falso de SCOTIABANK*

## Localización

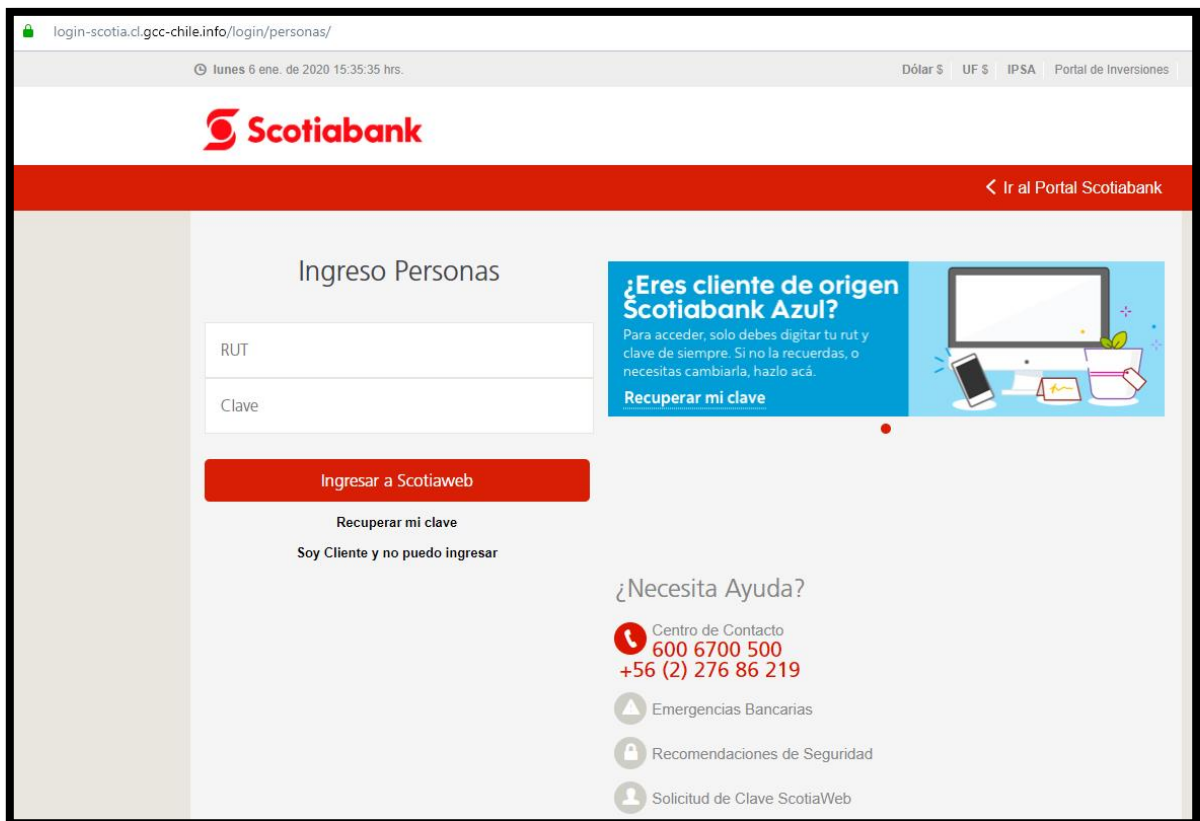
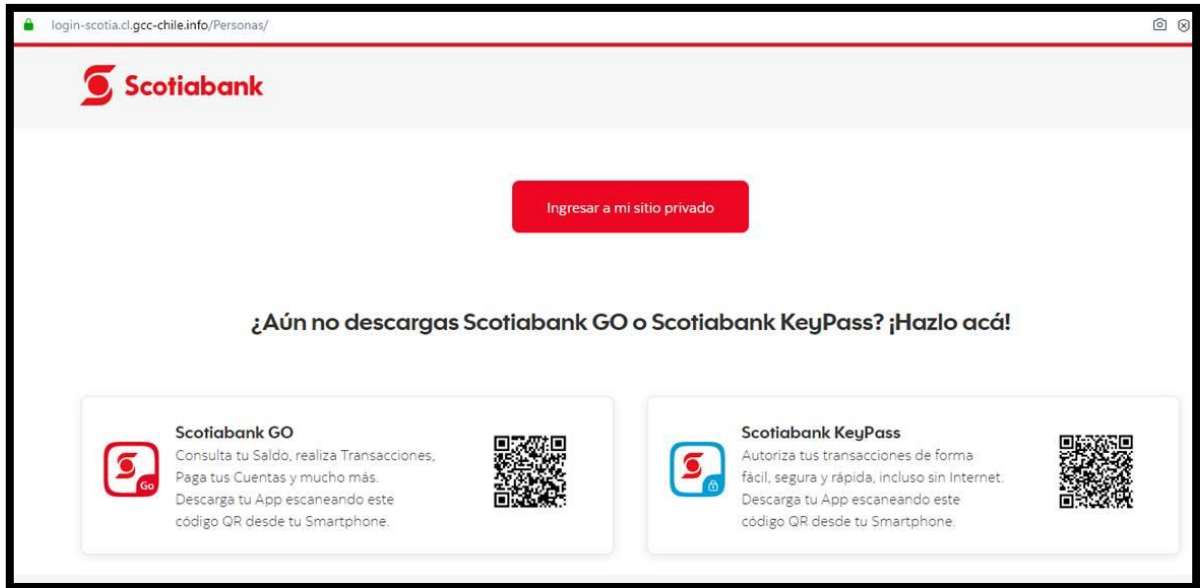
India, Bangalore, Karnataka

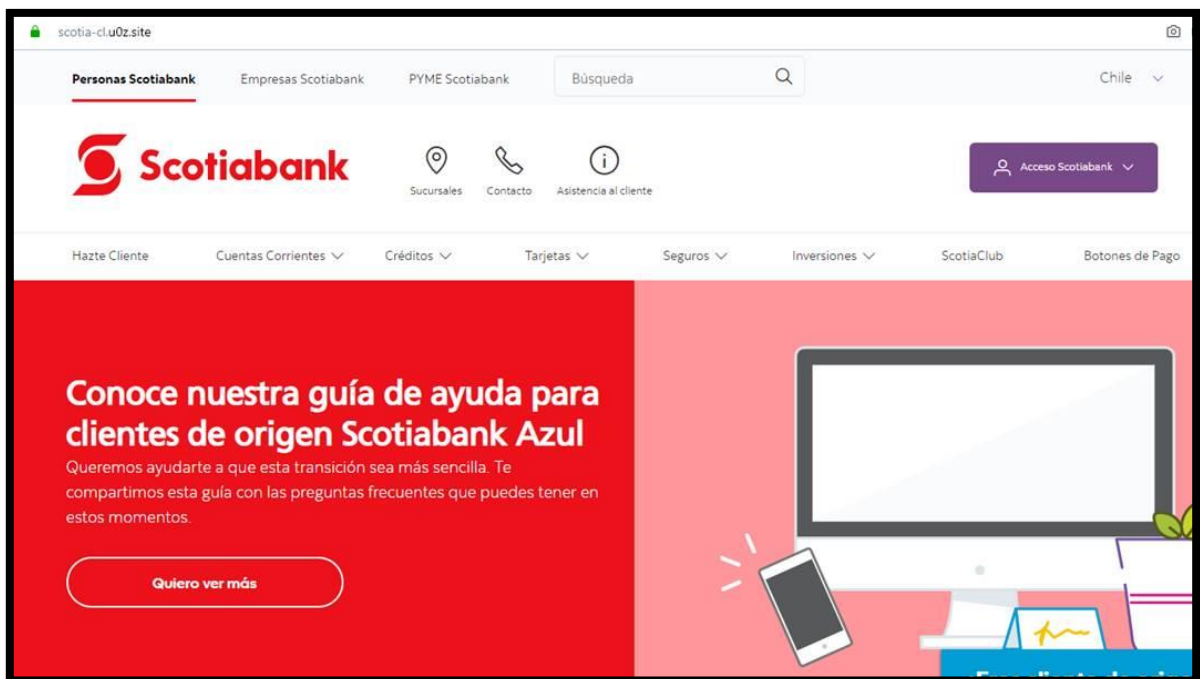
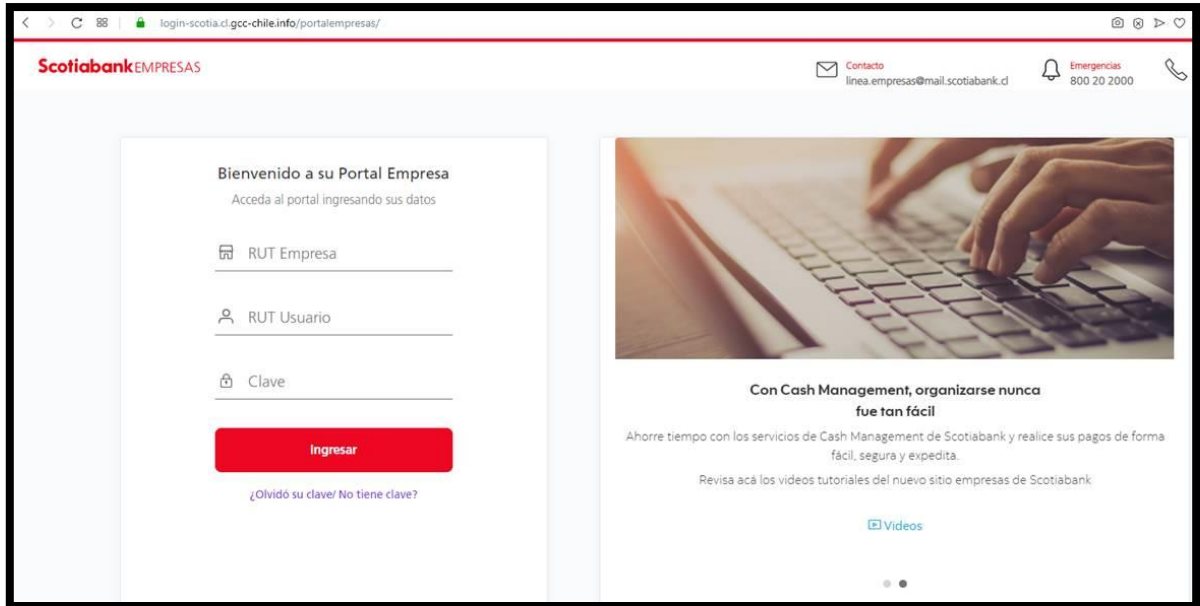


San Francisco, California, Estados Unidos




## Imagen del sitio






scotia-cl.u0z.site/Personas/





[Ingresar a mi sitio privado](#)

**¿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.




 **Contáctanos**


Contact Center  
600 6700 500

Mesa Central  
(562) 2692 6000

Soporte Empresas  
600 600 7800

 **Visítanos**


Casa Matriz Banco Scotiabank S.A. Av. Costanera Sur 2710.



scotia-cl.u0z.site/login/personas/

🕒 Lunes 6 ene. de 2020 10:28:06 hrs.

Dólar \$ | UF \$ | IPSA | [Portal de Inversiones](#)



[← Ir al Portal Scotiabank](#)

**Ingreso Personas**

[Ingresar a Scotiaweb](#)


[Recuperar mi clave](#)

Soy Cliente y no puedo ingresar


**¿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](#)



¿Necesita Ayuda?

 Centro de Contacto  
**600 6700 500**  
**+56 (2) 276 86 219**



scotia-cl.u0z.site/portalesempresas/

**Scotiabank**EMPRESAS

**Bienvenido a su Portal Empresa**  
Acceda al portal ingresando sus datos

**Ingresar**

[¿Olvidó su clave/ No tiene clave?](#)

## Whois

```
Domain Name: gcc-chile.info
Registrar WHOIS Server: whois.namesilo.com
Registrar URL: https://www.namesilo.com/
Updated Date: 2020-01-06T07:00:00Z
Creation Date: 2020-01-06T07:00:00Z
Registrar Registration Expiration Date: 2021-01-06T07:00:00Z
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-b6dc0191cd68608deaab5285delaalf9@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-b6dc0191cd68608deaab5285delaalf9@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-b6dc0191cd68608deaab5285delaalf9@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: 2020-01-06T07:00:00Z <<<

For more information on Whois status codes, please visit https://icann.org/epp

NOTICE AND TERMS OF USE: You are not authorized to access or query our WHOIS
database through the use of high-volume, automated, electronic processes. The
```

```
Domain name: u0z.site
Registry Domain ID: D150113626-CNIC
Registrar WHOIS Server: whois.namecheap.com
Registrar URL: http://www.namecheap.com
Updated Date: 0001-01-01T00:00:00.00Z
Creation Date: 2019-12-05T08:25:25.00Z
Registrar Registration Expiration Date: 2020-12-05T08:25:25.00Z
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
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: 64c8a8cbf7144228891437c30043749e.protect@whoisguard.com
Name Server: maeve.ns.cloudflare.com
Name Server: oswald.ns.cloudflare.com
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2020-01-06T02:14:11.39Z <<<
```

## 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.