

Alerta de seguridad informática	8FFR-00106-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	10 de Noviembre de 2019
Última revisión	10 de Noviembre de 2019

## NOTIFICACIÓN

La información consignada en el presente informe es producto del análisis de múltiples fuentes, de terceras partes e investigaciones 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 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 un portal fraudulento asociado a una IP que suplanta el sitio web oficial de **Banco Estado**, 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

[https://www\[.\]bancoestado\[.\]xyz/imagenes/comun2009/en-linea-personas\[.\]php](https://www[.]bancoestado[.]xyz/imagenes/comun2009/en-linea-personas[.]php)  
[http://scratchpad\[.\]co\[.\]in/owner/imagenes/comun2008/banca-en-linea-personas\[.\]html](http://scratchpad[.]co[.]in/owner/imagenes/comun2008/banca-en-linea-personas[.]html)  
[http://identitylampang\[.\]com/fonts/www\[.\]bancoestado\[.\]cl/imagenes/comun2008/banca-en-linea-personas\[.\]html](http://identitylampang[.]com/fonts/www[.]bancoestado[.]cl/imagenes/comun2008/banca-en-linea-personas[.]html)  
[https://www-portal-estado\[.\]ga/www\[.\]bancoestado\[.\]cl/](https://www-portal-estado[.]ga/www[.]bancoestado[.]cl/)

Domain <b>bancoestadoo.xyz</b> ⓘ																	
<b>bancoestadoo / xyz /</b>  <b>Subdomains</b>																	
record type	TTL	value															
<b>A</b>	7207	<a href="https://www[.]bancoestadoo[.]xyz">139.59.78.11</a>															
<b>NS</b>	172800	<a href="https://www[.]bancoestadoo[.]xyz">ns1.dnsowl.com</a>	 <b>Zones on DNS server</b> <a href="https://www[.]bancoestadoo[.]xyz">104.207.141.138, 198.251.84.16, 185.34.216.159</a>														
<b>NS</b>	172800	<a href="https://www[.]bancoestadoo[.]xyz">ns2.dnsowl.com</a>	 <b>Zones on DNS server</b> <a href="https://www[.]bancoestadoo[.]xyz">45.32.237.128, 168.235.75.52, 64.32.22.100</a>														
<b>NS</b>	172800	<a href="https://www[.]bancoestadoo[.]xyz">ns3.dnsowl.com</a>	 <b>Zones on DNS server</b> <a href="https://www[.]bancoestadoo[.]xyz">45.63.106.63, 209.141.39.150, 45.63.5.234</a>														
<b>SOA</b>	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>1573222199</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	1573222199	Refresh	7200	Retry	1800	Expire	1209600	Minimum TTL	600
Mname	ns1.dnsowl.com																
Rname	hostmaster.dnsowl.com																
Serial number	1573222199																
Refresh	7200																
Retry	1800																
Expire	1209600																
Minimum TTL	600																

Domain <b>scratchpad.co.in</b> ⓘ																	
<b>scratchpad / co / in /</b>  <b>Subdomains</b>																	
record type	TTL	value															
<b>A</b>	10800	<a href="https://www[.]scratchpad[.]co[.]in">166.62.28.89</a>															
<b>NS</b>	3600	<a href="https://www[.]scratchpad[.]co[.]in">ns59.domaincontrol.com</a>	 <b>Zones on DNS server</b> <a href="https://www[.]scratchpad[.]co[.]in">97.74.100.31</a>														
<b>NS</b>	3600	<a href="https://www[.]scratchpad[.]co[.]in">ns60.domaincontrol.com</a>	 <b>Zones on DNS server</b> <a href="https://www[.]scratchpad[.]co[.]in">173.201.68.31</a>														
<b>MX</b>	3600	<b>0 mail.scratchpad.co.in</b>															
<b>TXT</b>	3600	<b>v=spf1 a mx ptr include:secureserver.net ~all</b>															
<b>SOA</b>	3600	<table border="1"> <tr><td>Mname</td><td>ns59.domaincontrol.com</td></tr> <tr><td>Rname</td><td>dns.jomax.net</td></tr> <tr><td>Serial number</td><td>2019031802</td></tr> <tr><td>Refresh</td><td>28800</td></tr> <tr><td>Retry</td><td>7200</td></tr> <tr><td>Expire</td><td>604800</td></tr> <tr><td>Minimum TTL</td><td>600</td></tr> </table>		Mname	ns59.domaincontrol.com	Rname	dns.jomax.net	Serial number	2019031802	Refresh	28800	Retry	7200	Expire	604800	Minimum TTL	600
Mname	ns59.domaincontrol.com																
Rname	dns.jomax.net																
Serial number	2019031802																
Refresh	28800																
Retry	7200																
Expire	604800																
Minimum TTL	600																

Domain identitylampang.com ⓘ			
identitylampang / com /  Subdomains			
record type	TTL	value	
A	14400	27.254.174.60	
NS	14400	<a href="#">In30.hostingdynamo.net</a>	 Zones on DNS server 27.254.174.60
NS	14400	<a href="#">In29.hostingdynamo.net</a>	 Zones on DNS server 27.254.174.60
MX	14400	10 mail.identitylampang.com 27.254.174.60	
TXT	14400	v=spf1 a mx ip4:27.254.174.60 ~all	
SOA	14400	Mname	In29.hostingdynamo.net
		Rname	hostmaster.identitylampang.com
		Serial number	2019050201
		Refresh	14400
		Retry	3600
		Expire	1209600
		Minimum TTL	86400






Domain www-portal-estado.ga ⓘ			
www-portal-estado / ga /  Subdomains			
record type	TTL	value	
A	3600	91.209.70.108	
NS	300	<a href="#">ns04.freenom.com</a>	 Zones on DNS server 104.155.29.241
NS	300	<a href="#">ns01.freenom.com</a>	 Zones on DNS server 54.171.131.39
NS	300	<a href="#">ns02.freenom.com</a>	 Zones on DNS server 52.19.156.76
NS	300	<a href="#">ns03.freenom.com</a>	 Zones on DNS server 104.155.27.112
SOA	300	Mname	ns01.freenom.com
		Rname	soa.freenom.com
		Serial number	1572996918
		Refresh	10800
		Retry	3600
		Expire	604800
		Minimum TTL	3600

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

## Certificado

Criteria		Identity = 'www.bancoestadoo.xyz'			
Certificates	<a href="#">crt.sh ID</a>	<a href="#">Logged At</a> ⓘ	<a href="#">Not Before</a>	<a href="#">Not After</a>	<a href="#">Issuer Name</a>
	<a href="#">2086828581</a>	2019-11-08	2019-11-08	2020-02-06	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	<a href="#">2086828670</a>	2019-11-08	2019-11-08	2020-02-06	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3

<b>Criteria</b>	Identity = 'scratchpad.co.in'
<b>Certificates</b>	None found

<b>Criteria</b>		Identity = 'identitylampang.com'			
<b>Certificates</b>	<a href="#">crt.sh ID</a>	<a href="#">Logged At</a>	<a href="#">Not Before</a>	<a href="#">Not After</a>	<a href="#">Issuer Name</a>
	<a href="#">2064388322</a>	2019-11-02	2019-11-02	2020-01-31	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	<a href="#">2064388227</a>	2019-11-02	2019-11-02	2020-01-31	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	<a href="#">1861021205</a>	2019-09-03	2019-09-03	2019-12-02	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	<a href="#">1841967215</a>	2019-09-03	2019-09-03	2019-12-02	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	<a href="#">1654887590</a>	2019-07-05	2019-07-05	2019-10-03	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	<a href="#">1642011854</a>	2019-07-05	2019-07-05	2019-10-03	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3

<b>Criteria</b>		Identity = 'www-portal-estado.ga'			
<b>Certificates</b>	<a href="#">crt.sh ID</a>	<a href="#">Logged At</a>	<a href="#">Not Before</a>	<a href="#">Not After</a>	<a href="#">Issuer Name</a>
	<a href="#">2077121845</a>	2019-11-06	2019-11-06	2020-02-04	C=US, ST=TX, L=Houston, O="cPanel, Inc.", CN="cPanel, Inc. Certification Authority"
	<a href="#">2077120906</a>	2019-11-06	2019-11-06	2020-02-04	C=US, ST=TX, L=Houston, O="cPanel, Inc.", CN="cPanel, Inc. Certification Authority"

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
















**IP's**




- 139[.]59[.]78[.]11
- 166[.]62[.]28[.]89
- 27[.]254[.]174[.]60
- 91[.]209[.]70[.]108

**Domain bancoestadoo.xyz is located on IP address**

**<< 139.59.78.11 >>**

<b>Block start</b>	139.59.0.0
<b>End of block</b>	139.59.255.254
<b>Block size</b>	65535  Domains in block
<b>Block name</b>	DIGITALOCEAN-AP
<b>AS number</b>	<a href="#">14061</a>
<b>Parent block</b>	<a href="#">139.59.0.0 - 139.59.255.255</a>
<b>Organization</b>	<a href="#">DigitalOcean, LLC</a>
<b>Country</b>	SG , Singapore
<b>Host name</b>	no record in reverse zone
<b>Domains</b>	1 <a href="#">bancoestadoo.xyz</a>

Domain <u>scratchpad.co.in</u> is located on IP address ≤≤ 166.62.28.89 ≥≥	
Block start	166.62.0.0
End of block	166.62.127.255
Block size	32768  Domains in block
Block name	GO-DADDY-COM-LLC
AS number	26496
Parent block	166.0.0.0 - 166.255.255.255
Organization	GoDaddy.com, LLC
City	Scottsdale
Region/State	Arizona
Country	 US , United States
Reg. date	2012-11-14
Host name	ip-166-62-28-89.ip.secureserver.net
Web server	Apache/2.4.23
Domain count	>= 2660  Servers around
Domains	<ol style="list-style-type: none"> <li>1  <a href="#">*.grabiphone.com</a></li> <li>2  <a href="#">*.vinej.com</a></li> <li>3  <a href="#">03239999999.com</a></li> <li>4  <a href="#">0791studios.com</a></li> <li>5  <a href="#">091trends.com</a></li> <li>6  <a href="#">101godrej.in</a></li> <li>7  <a href="#">10dlkar.com</a></li> <li>8  <a href="#">1234tv.ml</a></li> <li>9  <a href="#">22itc.com</a></li> <li>10  <a href="#">2stechno.com</a></li> <li>11  <a href="#">365-topazmike-one.info</a></li> <li>12  <a href="#">365topazjohntwo.info</a></li> </ol>

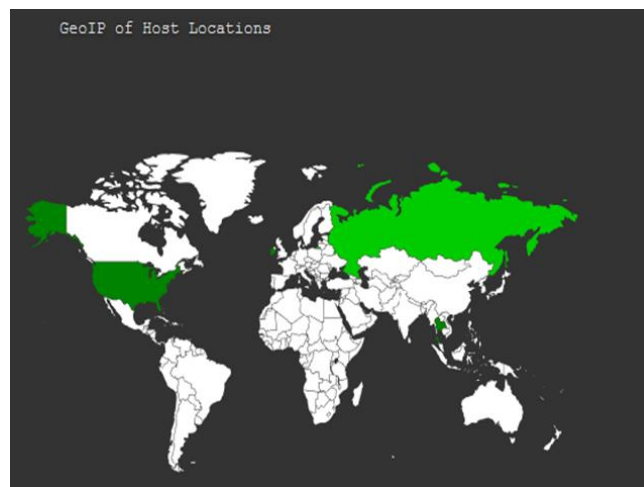
Domain <u>identitylampang.com</u> is located on IP address ≤≤ 27.254.174.60 ≥≥	
Block start	27.254.174.0
End of block	27.254.174.255
Block size	256  Domains in block
Block name	idc-csloxinfo
AS number	9891
Parent block	27.254.0.0 - 27.254.255.255
Organization	reassign to "CSLOXINFO-IDC" contact *
City	Bangkok
Region/State	Krung Thep Maha Nakhon
Country	 TH , Thailand
Host name	In29.hostingdynamo.net
Domains	1  <a href="#">identitylampang.com</a>

<b>Domain <u>www-portal-estado.ga</u> is located on IP address &lt;&lt; 91.209.70.108 &gt;&gt;</b>	
<b>Block start</b>	91.209.70.0
<b>End of block</b>	91.209.70.255
<b>Block size</b>	256  Domains in block
<b>Block name</b>	PIHLTD
<b>AS number</b>	<a href="#">43317</a>
<b>Parent block</b>	<a href="#">91.0.0.0 - 91.255.255.255</a>
<b>Organization</b>	<a href="#">ORG-PIHL2-RIPE</a>
<b>City</b>	Moscow
<b>Region/State</b>	Moskva
<b>Country</b>	 RU , Russian Federation
<b>Reg. date</b>	2008-10-29
<b>Host name</b>	no record in reverse zone
<b>Domains</b>	1   <a href="#">www-portal-estado.ga</a>

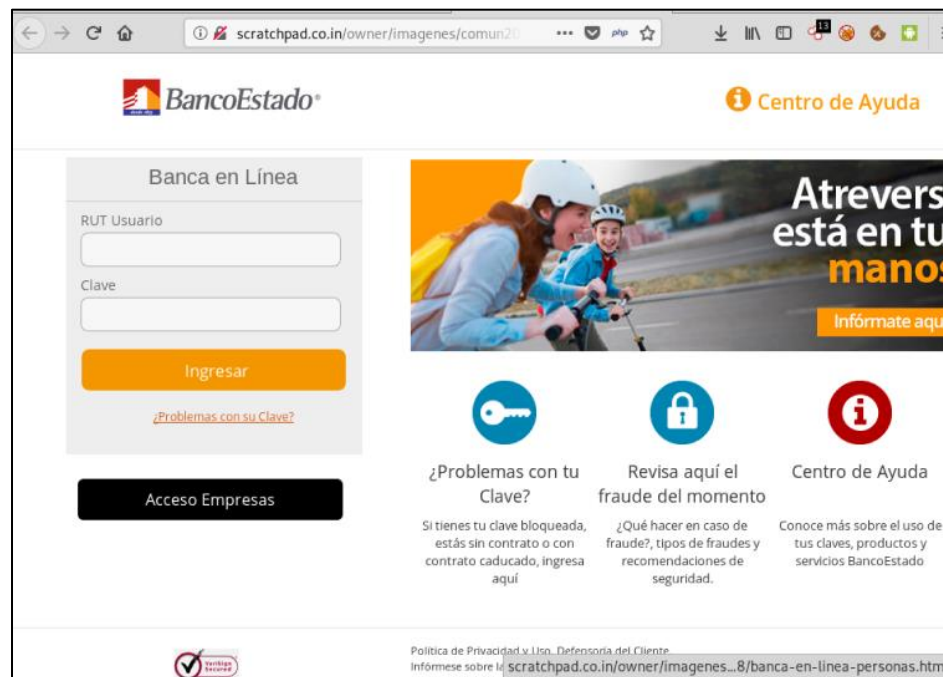
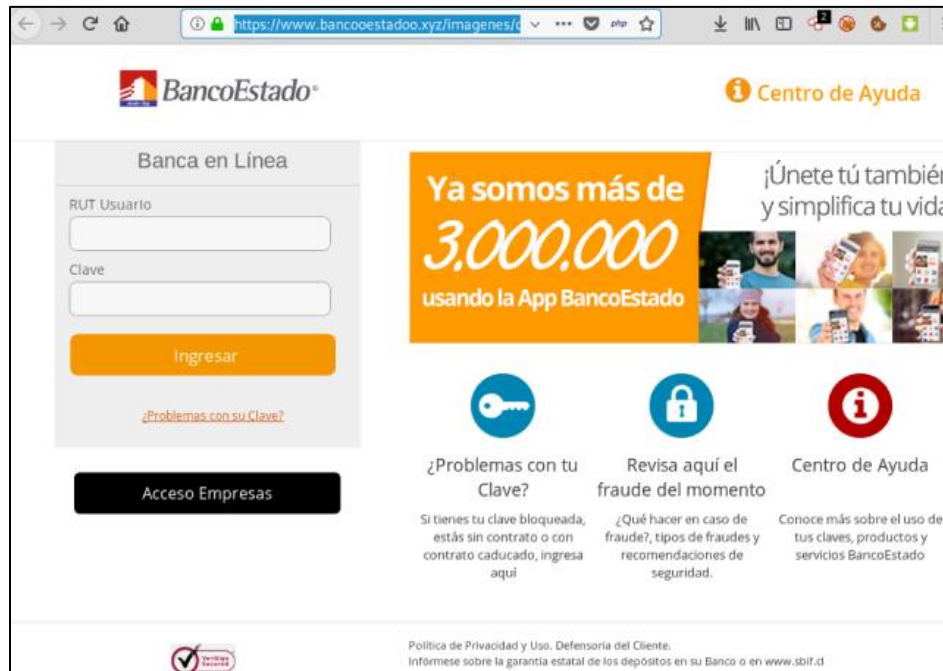
Ilustración 3 Ip de Origen donde se aloja Sitio Falso del Banco Estado

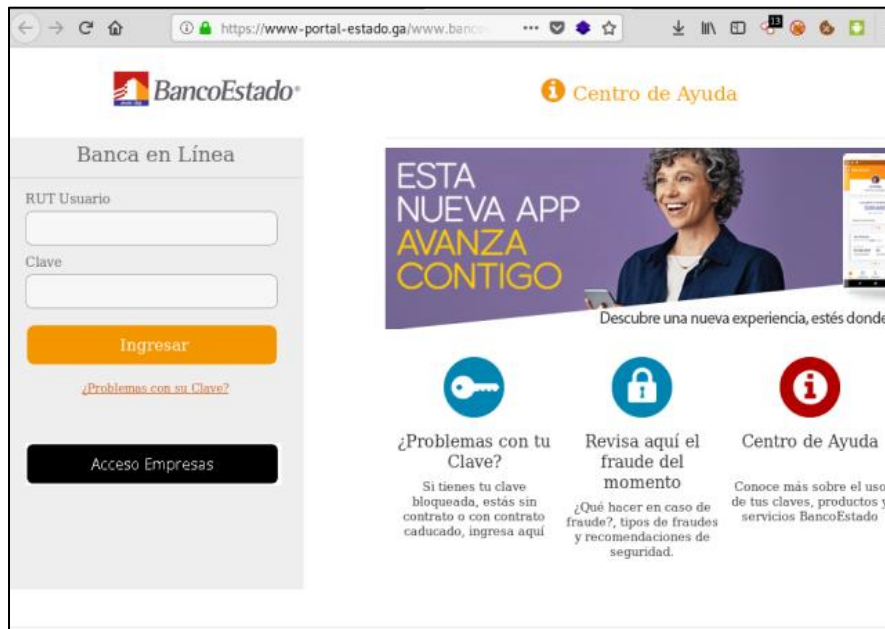
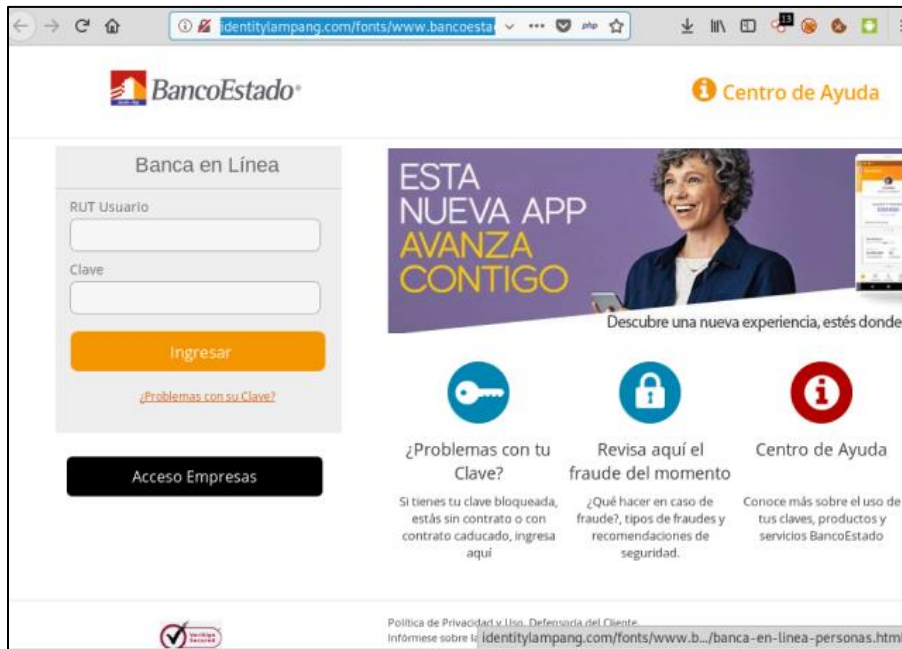
### Localización

Singapur / Arizona, Esatdos Unidos / Bangkok, Tailandia / Moscú, Federación Rusa



Imagen







## Whois

```
Domain Name: bancoestadoo.xyz
Registrar WHOIS Server: whois.namesilo.com
Registrar URL: https://www.namesilo.com/
Updated Date: 2019-11-08T07:00:00Z
Creation Date: 2019-11-08T07:00:00Z
Registrar Registration Expiration Date: 2020-11-08T07:00:00Z
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-3ed0be36d8668dcabllcd26056f04ba4@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-3ed0be36d8668dcabllcd26056f04ba4@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-3ed0be36d8668dcabllcd26056f04ba4@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: 2019-11-08T07:00:00Z <<<

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

```
Domain Name: scratchpad.co.in
Registry Domain ID: D41440000005735521-IN
Registrar WHOIS Server:
Registrar URL: www.godaddy.com
Updated Date: 2019-03-23T18:20:02Z
Creation Date: 2018-03-06T07:36:43Z
Registry Expiry Date: 2020-03-06T07:36:43Z
Registrar: GoDaddy.com, LLC
Registrar IANA ID: 146
Registrar Abuse Contact Email:
Registrar Abuse Contact Phone:
Domain Status: clientUpdateProhibited http://www.icann.org/epp#clientUpdateProhibited
Domain Status: clientDeleteProhibited http://www.icann.org/epp#clientDeleteProhibited
Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited
Domain Status: clientRenewProhibited http://www.icann.org/epp#clientRenewProhibited
Registry Registrant ID:
Registrant Name:
Registrant Organization:
Registrant Street:
Registrant Street:
Registrant Street:
Registrant City:
Registrant State/Province: Karnataka
Registrant Postal Code:
Registrant Country: IN
Registrant Phone:
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: Please contact the Registrar listed above
Registry Admin ID:
Admin Name:
Admin Organization:
Admin Street:
Admin Street:
Admin Street:
Admin City:
Admin State/Province:
Admin Postal Code:
Admin Country:
Admin Phone:
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: Please contact the Registrar listed above
Registry Tech ID:
Tech Name:
Tech Organization:
Tech Street:
Tech Street:
Tech Street:
Tech City:
Tech State/Province:
Tech Postal Code:
Tech Country:
Tech Phone:
Tech Phone Ext:
Tech Fax:
Tech Fax Ext:
Tech Email: Please contact the Registrar listed above
Name Server: ns59.domaincontrol.com
Name Server: ns60.domaincontrol.com
```

```
Domain Name: IDENTITYLAMPANG.COM
Registry Domain ID: 2386633424 DOMAIN COM-VRSN
Registrar WHOIS Server: whois.publicdomainregistry.com
Registrar URL: www.publicdomainregistry.com
Updated Date: 2019-07-02T02:21:51Z
Creation Date: 2019-05-02T03:29:22Z
Registrar Registration Expiration Date: 2020-05-02T03:29:22Z
Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com
Registrar IANA ID: 303
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Registry Registrant ID: Not Available From Registry
Registrant Name: Ratthasit Yajor
Registrant Organization: Ratthasit Yajor
Registrant Street: 173 0
Registrant City: Muang
Registrant State/Province: Lampang
Registrant Postal Code: 52100
Registrant Country: TH
Registrant Phone: +66.810305262
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: ratthasit.it@gmail.com
Registry Admin ID: Not Available From Registry
Admin Name: Ratthasit Yajor
Admin Organization: Ratthasit Yajor
Admin Street: 173 0
Admin City: Muang
Admin State/Province: Lampang
Admin Postal Code: 52100
Admin Country: TH
Admin Phone: +66.810305262
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: ratthasit.it@gmail.com
Registry Tech ID: Not Available From Registry
Tech Name: Ratthasit Yajor
Tech Organization: Ratthasit Yajor
Tech Street: 173 0
Tech City: Muang
Tech State/Province: Lampang
Tech Postal Code: 52100
Tech Country: TH
Tech Phone: +66.810305262
Tech Phone Ext:
Tech Fax:
Tech Fax Ext:
Tech Email: ratthasit.it@gmail.com
Name Server: ln29.hostingdynamo.net
Name Server: ln30.hostingdynamo.net
DNSSEC: Unsigned
Registrar Abuse Contact Email: abuse-contact@publicdomainregistry.com
Registrar Abuse Contact Phone: +1.2013775952
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2019-11-08T14:27:40Z <<<
```

```
root@gsa:~# whois -I www-portal-estado.ga
% IANA WHOIS server
% for more information on IANA, visit http://www.iana.org
% This query returned 1 object

domain:          GA

organisation:    Agence Nationale des Infrastructures Numériques et des Fréquences (ANINF)
address:         Cours Pasteur, (Immeuble de la Solde)
address:         BP: 798
address:         Libreville
address:         Gabon

contact:         administrative
name:            TLD Admin Contact
organisation:    Agence Nationale des Infrastructures Numériques et des Fréquences (ANINF)
address:         Cours Pasteur, (Immeuble de la Solde)
address:         BP: 798
address:         Libreville
address:         Gabon
phone:           +241 01 76 32 49
e-mail:          cctldga-admin@nic.ga

contact:         technical
name:            Manager ICT
organisation:    Agence Nationale des Infrastructures Numériques et des Fréquences (ANINF)
address:         Cours Pasteur, (Immeuble de la Solde)
address:         BP: 798
address:         Libreville
address:         Gabon
phone:           +241 01 76 32 49
e-mail:          cctldga-tech@nic.ga

nserver:        A.NS.GA 185.21.168.49 2a04:1b00:c:0:0:0:0:1
nserver:        B.NS.GA 185.21.169.49 2a04:1b00:d:0:0:0:0:1
nserver:        C.NS.GA 185.21.170.49 2a04:1b00:e:0:0:0:0:1
nserver:        D.NS.GA 185.21.171.49 2a04:1b00:f:0:0:0:0:1
```

## 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