Alerta de seguridad informática	8FFR-00169-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	31 de diciembre de 2019
Última revisión	31 de diciembre 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 fraudulentos asociados a tres IP que suplantan el sitio web oficial de Banco Estado, 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

www[.]aisgwb[.]org/css/user/imagenes/comun2008/banca-en-linea-personas[.]html
www[.]banco-estadocl[.]xyz/imagenes/comun2008/banca-en-linea-personas[.]php?html
bloqueo-ban0oestad0[.]ddns[.]net/www[.]bancoestado[.]cl[.]bloqueo/

Domain aisgwb.org

aisgwb / org / Subdomains

record type	TTL	value		
A	14400	132.148.151.253		
NS	86400	ns1.aisgwb.org	Zones on DNS server	132.148.151.253
NS	86400	ns2.aisgwb.org	Zones on DNS server	132.148.151.253
MX	14400	0 aisgwb.org		
TXT	14400	v=spf1 +a +mx +ip4:10.193.82.71 ~all		

SOA	86400	Mname	ns1.secureserver.net
		Rname	info.dtechsystem.net
		Serial number	2019111903
		Refresh	3600
		Retry	1800
		Expire	1209600
		Minimum TTL	86400

Domain banco-estadocl.xyz

banco-estadocl / xyz / Subdomains

record type	TTL	value		
A	7207	206.189.137.123		
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, 45.32.237.128, 64.32.22.100
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	1577712626
		Refresh	7200
		Retry	1800
		Expire	1209600
		Minimum TTL	600

Domain bloqueo-ban0oestad0.ddns.net

bloqueo-ban0oestad0 / ddns / net / Subdomains

record type	TTL	value	
A	60	178.159.36.146	

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

Certificados

Criteria	Identity = 'www.aisgwb.org'; Exclude expired certificates

Certificates

crt.sh ID	Logged At	Not Before	Not After	Issuer Name
2129291511	2019-11-19	2019-11-19	2020-02-17	C=US, ST=TX, L=Houston, O="cPanel, Inc.", CN="cPanel, Inc. Certification Authority"
2129291252	2019-11-19	2019-11-19	2020-02-17	C=US, ST=TX, L=Houston, O="cPanel, Inc.", CN="cPanel, Inc. Certification Authority"
1975979641	2019-10-09	2019-10-09	2020-01-07	C=US, ST=TX, L=Houston, O="cPanel, Inc.", CN="cPanel, Inc. Certification Authority"
1975979288	2019-10-09	2019-10-09	2020-01-07	C=US, ST=TX, L=Houston, O="cPanel, Inc.", CN="cPanel, Inc. Certification Authority"

Subject DN	CN=www.banco-estadocl.xyz
Issuer DN	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
Serial	278442828511745924721375145638121951438143
Validity	2019-12-29 02:07:04 **to** 2020-03-28 02:07:04 (90 days, 0:00:00)
Names	www.banco-estadocl.xyz

Subject DN	CN=bloqueo-ban0oestad0.ddns.net
Issuer DN	C=US, ST=TX, L=Houston, O=cPanel, Inc., CN=cPanel, Inc. Certification Authority
Serial	252802407543064944847981493396171400459
Validity	2019-12-30 00:00:00 **to** 2020-03-29 23:59:59 (90 days, 23:59:59)
Names	bloqueo-ban0oestad0.ddns.net cpanel.bloqueo-ban0oestad0.ddns.net mail.bloqueo-ban0oestad0.ddns.net webdisk.bloqueo-ban0oestad0.ddns.net webmail.bloqueo-ban0oestad0.ddns.net www.bloqueo-ban0oestad0.ddns.net

Ilustración 2 Certificado Utilizado en Url del sitio Falso de BANCOESTADO

IP

132[.]148[.]151[.]253
206[.]189[.]137[.]123
178[.]159[.]36[.]146

Domain aisgwb.org is located on IP address << 132.148.151.253 >>	
Block start	132.148.0.0
End of block	132.148.255.255
Block size	65536 Domains in block
Block name	GO-DADDY-COM-LLC
AS number	26496
Parent block	132.0.0.0 - 132.255.255.255
Organization	GoDaddy.com, LLC
City	Scottsdale
Region/State	Arizona
Country	US , United States
Reg. date	2015-10-21
Host name	ip-132-148-151-253.ip.secureserver.net
Domain count	>= 5 Servers around
Domains	1 aisgwb.org 2 iphk.in 3 powerlinetechnocrats.com 4 sinteredglassware.com 5 www.hospiquip.com

Domain banco-estadocl.xyz is located on IP address << 206.189.137.123 >>

Block start	206.189.0.0
End of block	206.189.255.255
Block size	65536 Domains in block
Block name	PILOT-NETBLK-3
AS number	14061
Parent block	206.0.0.0 - 206.255.255.255
Organization	Pilot Network Services, Inc
City	Alameda
Region/State	California
Country	US , United States
Reg. date	1995-11-15
Host name	no record in reverse zone
Domains	1 banco-estadocl.xyz

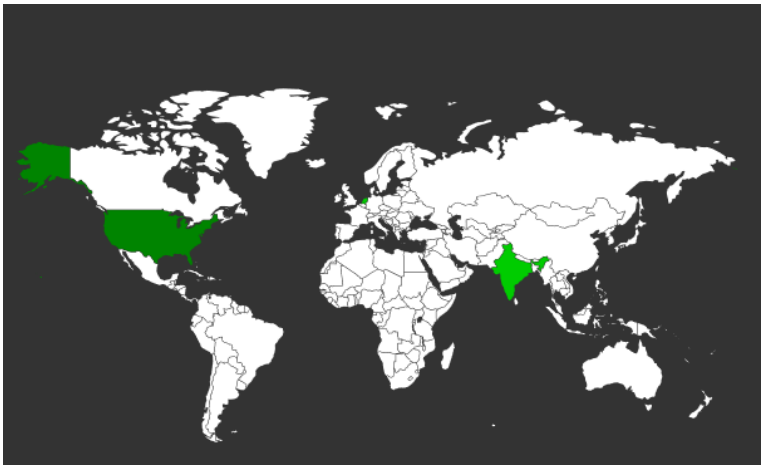
Domain bloqueo-ban0oestad0.ddns.net is located on IP address << 178.159.36.146 >>

Block start	178.159.36.0
End of block	178.159.36.255
Block size	256 Domains in block
Block name	PrivateInternetHosting
AS number	48666
Parent block	178.0.0.0 - 178.255.255.255
Organization	ORG-PIHL2-RIPE
City	Moscow
Region/State	Moskva
Country	RU , Russian Federation
Reg. date	2010-08-25
Host name	no record in reverse zone
Domain count	>= 3 Servers around
Domains	1 bloqueo-ban0oestad0.ddns.net 2 simular-avance-cl-chile.club 3 www.l0gin-banc0chile.xyz

Ilustración 3 Ip de Origen donde se aloja Sitio Falso de BANCOESTADO

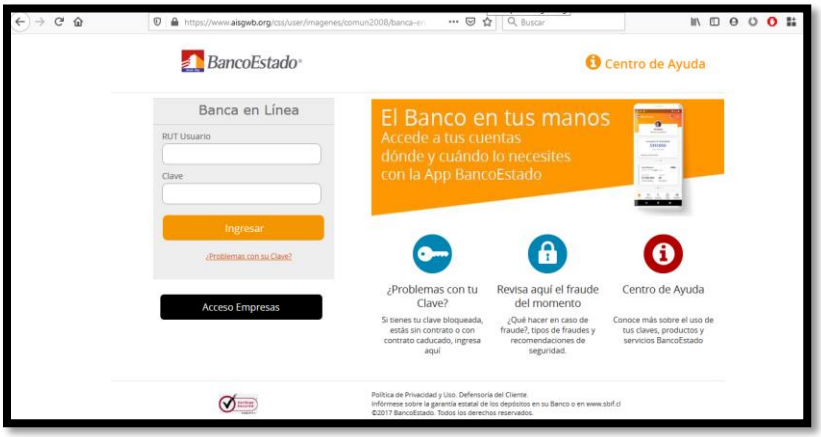
Localización

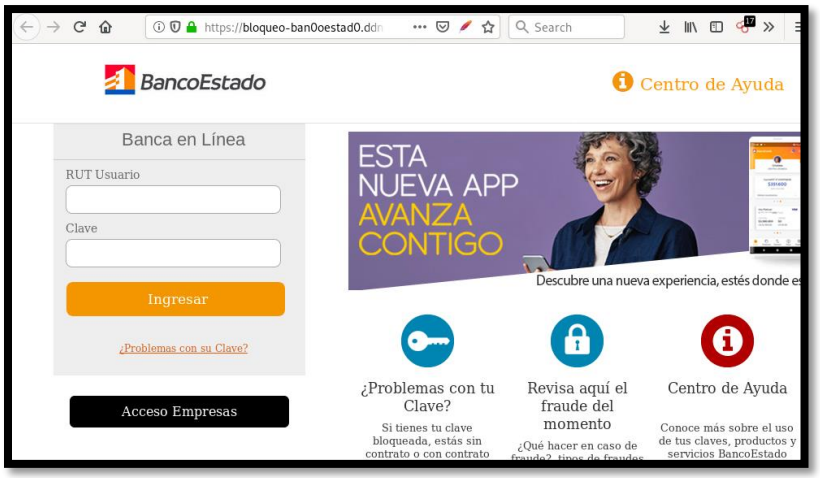
Scottsdale, Arizona, Estados Unidos
Bangalore, Karnataka, India



Moscú, Moscú, Rusia

Imagen del sitio





Whois

```
Domain Name: AISGWB.ORG
Registry Domain ID: D168461833-LROR
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: http://www.godaddy.com
Updated Date: 2019-04-19T07:10:13Z
Creation Date: 2013-04-17T10:50:10Z
Registrar Registration Expiration Date: 2020-04-17T10:50:10Z
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: DTECH SYSTEM
Registrant State/Province: West Bengal
Registrant Country: IN
Registrant Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=AISGWB.ORG
Admin Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=AISGWB.ORG
Tech Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=AISGWB.ORG
Name Server: NS1.AISGWB.ORG
Name Server: NS2.AISGWB.ORG
DNSSEC: unsigned
```

```
Domain Name: BANCO-ESTADOCL.XYZ
Registry Domain ID: D156882506-CNIC
Registrar WHOIS Server: whois.namesilo.com
Registrar URL: https://www.namesilo.com
Updated Date: 2019-12-29T00:30:08.0Z
Creation Date: 2019-12-29T00:25:38.0Z
Registry Expiry Date: 2020-12-29T23:59:59.0Z
Registrar: NameSilo, LLC
Registrar IANA ID: 1479
Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: addPeriod https://icann.org/epp#addPeriod
Registrant Organization: See PrivacyGuardian.org
Registrant State/Province: AZ
Registrant Country: US
Registrant Email: Please query the RDDS service of the Registrar of Record identified in this output for infor
mation on how to contact the Registrant, Admin, or Tech contact of the queried domain name.
Admin Email: Please query the RDDS service of the Registrar of Record identified in this output for informatio
n on how to contact the Registrant, Admin, or Tech contact of the queried domain name.
Tech Email: Please query the RDDS service of the Registrar of Record identified in this output for information
 on how to contact the Registrant, Admin, or Tech contact of the queried domain name.
Name Server: NS1.DNSOWL.COM
Name Server: NS2.DNSOWL.COM
Name Server: NS3.DNSOWL.COM
DNSSEC: unsigned
```

```
Domain Name: ddns.net
Registry Domain ID: 73816572_DOMAIN_NET-VRSN
Registrar WHOIS Server: whois.srsplus.com
Registrar URL: http://srsplus.com
Updated Date: 2019-04-01T15:03:00Z
Creation Date: 2001-06-28T16:04:59Z
Registrar Registration Expiration Date: 2020-06-28T16:04:59Z
Registrar: TLDS LLC. d/b/a SRSPlus
Registrar IANA ID: 320
Reseller:
Domain Status: clientTransferProhibited http://icann.org/epp#clientTransferProhibited
Registry Registrant ID:
Registrant Name: Dan Durrer
Registrant Organization: No-IP.com
Registrant Street: 425 Maestro  Dr. Second Floor
Registrant City: Reno
Registrant State/Province: NV
Registrant Postal Code: 89511
Registrant Country: US
Registrant Phone: +1.7758531883
Registrant Phone Ext.:
Registrant Fax:
Registrant Fax Ext.:
Registrant Email: domains@no-ip.com
Registry Admin ID:
Admin Name: Dan Durrer
Admin Organization: No-IP.com
Admin Street: 425 Maestro  Dr. Second Floor
Admin City: Reno
Admin State/Province: NV
Admin Postal Code: 89511
Admin Country: US
Admin Phone: +1.7758531883
Admin Phone Ext.:
Admin Fax:
Admin Fax Ext.:
Admin Email: domains@no-ip.com
Registry Tech ID:
Tech Name: Dan Durrer
Tech Organization: No-IP.com
Tech Street: 425 Maestro  Dr. Second Floor
Tech City: Reno
Tech State/Province: NV
Tech Postal Code: 89511
Tech Country: US
Tech Phone: +1.7758531883
Tech Phone Ext.:
Tech Fax:
Tech Fax Ext.:
Tech Email: domains@no-ip.com
Name Server: nf2.no-ip.com
Name Server: nf1.no-ip.com
Name Server: nf4.no-ip.com
Name Server: nf3.no-ip.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.