Alerta de seguridad informática	8FFR-00114-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	17 de Noviembre de 2019
Última revisión	17 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 dos portales fraudulentos asociados a una IP que suplantan 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

http[://]identitylampang[.]com/include/www[.]bancoestado[.]cl/imagenes/comun2008/banca-en-linea-personas[.]html

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

Domain identitylampang.com

identitylampang / com / Subdomains

d	TTL	value		
	14400	27.254.174.60		
	14400	ln30.hostingdynamo.net	Zones on DNS server	27.254.174.60
	14400	ln29.hostingdynamo.net	Zones on DNS server	27.254.174.60
	14400	10 mail.identitylampang.com		27.254.174.60
	14400	v=spf1 a mx ip4:27.254.174.60 ~all		

14400	Mname	ln29.hostingdynamo.net
	Rname	hostmaster.identitylampang.com
	Serial number	2019050201
	Refresh	14400
	Retry	3600
	Expire	1209600
	Minimum TTL	86400

Domain bancooesstado.xyz

bancooesstado / xyz / Subdomains

record type	TTL	value		
A	7207	139.59.3.13		
NS	172800	ns1.dnsowl.com	Zones on DNS server	198.251.84.16, 185.34.216.159, 104.207.141.138
NS	172800	ns2.dnsowl.com	Zones on DNS server	64.32.22.100, 168.235.75.52, 45.32.237.128
NS	172800	ns3.dnsowl.com	Zones on DNS server	209.141.39.150, 45.63.106.63, 45.63.5.234

SOA	172800	Mname	ns1.dnsowl.com
		Rname	hostmaster.dnsowl.com
		Serial number	1573759208
		Refresh	7200
		Retry	1800
		Expire	1209600
		Minimum TTL	600

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

Certificado

Criteria	Identity = 'identitylampang.com'

Certificates

crt.sh ID	Logged At ⇧	Not Before	Not After	Issuer Name
2064388322	2019-11-02	2019-11-02	2020-01-31	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
2064388227	2019-11-02	2019-11-02	2020-01-31	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1861021205	2019-09-03	2019-09-03	2019-12-02	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1841967215	2019-09-03	2019-09-03	2019-12-02	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1654887590	2019-07-05	2019-07-05	2019-10-03	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1642011854	2019-07-05	2019-07-05	2019-10-03	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3

Subject DN	CN=www.bancooesstado.xyz
Issuer DN	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
Serial	383415158210539448643098474701013258674648
Validity	2019-11-14 18:05:30 **to** 2020-02-12 18:05:30 (90 days, 0:00:00)
Names	www.bancooesstado.xyz

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

IP´s

27.254.174.60

139.59.3.13

Domain identitylampang.com 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	ln29.hostingdynamo.net

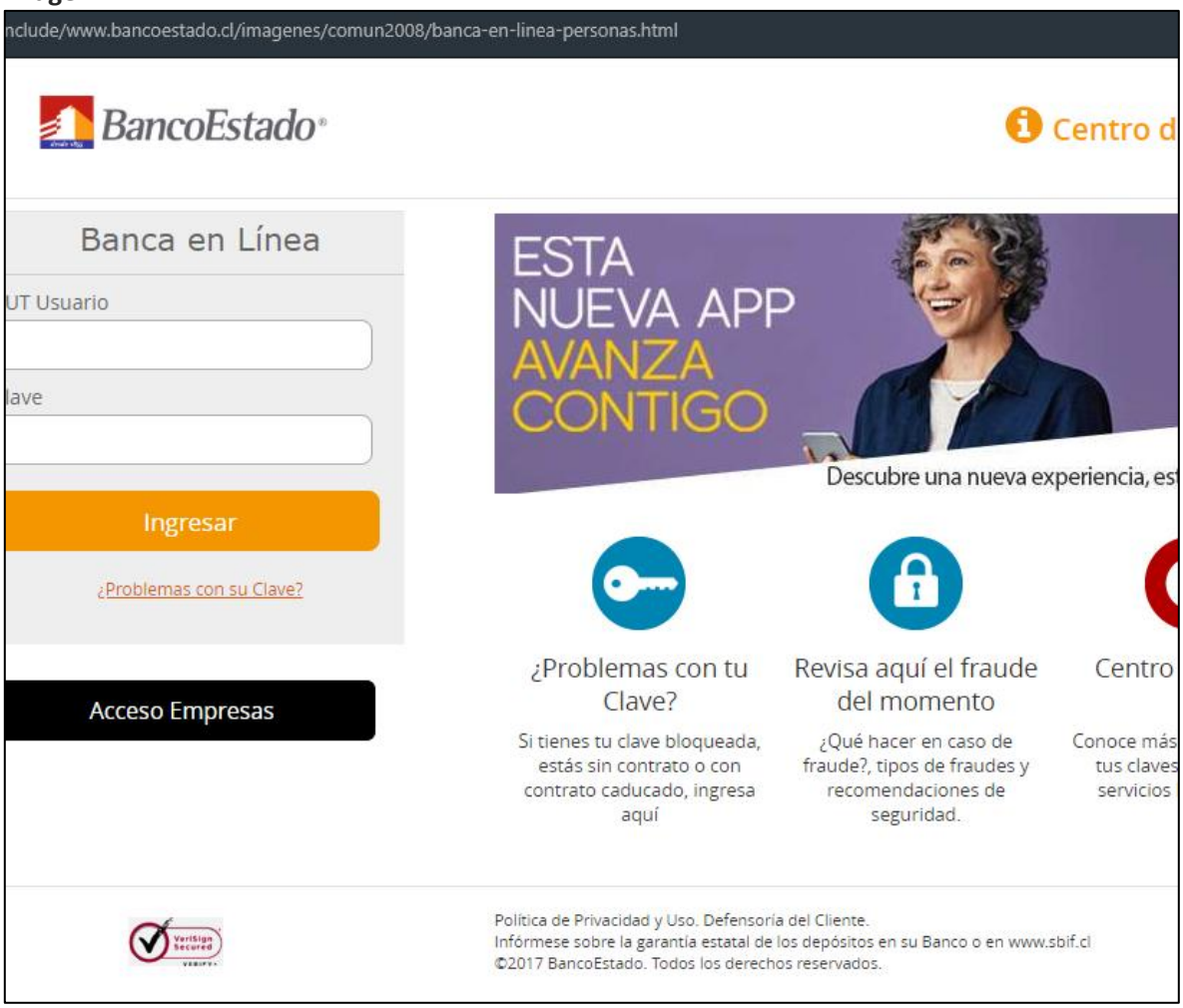
Domain bancooesstado.xyz is located on IP address << 139.59.3.13 >>	
Block start	139.59.0.0
End of block	139.59.255.254
Block size	65535 Domains in block
Block name	DIGITALOCEAN-AP
AS number	14061
Parent block	139.59.0.0 - 139.59.255.255
Organization	DigitalOcean, LLC
Country	SG , Singapore
Host name	no record
Web server	Apache/2.4.7(Ubuntu)
Powered by	PHP/5.5.9-1ubuntu4.19
Domain count	>= 2 Servers around

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

Localización

Bangkok, Krung Thep Maha Nakhon, Tailandia
Bangalore, Karnataka, India

Imagen


nclude/www.bancoestado.cl/imagenes/comun2008/banca-en-linea-personas.html
BancoEstado
Centro d
Banca en Línea
UT Usuario
lave
Ingresar
¿Problemas con su Clave?
Acceso Empresas
ESTA NUEVA APP AVANZA CONTIGO
Descubre una nueva experiencia, est
¿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
Conoce más tus claves servicios
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: 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#clientTransferProh
ibited
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: 2019-11-14T15:51:07Z <<<

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

Registration Service Provided By: HOSTINGDYNAMO.COM
```

```
Domain Name: bancooesstado.xyz
Registrar WHOIS Server: whois.namesilo.com
Registrar URL: https://www.namesilo.com/
Updated Date: 2019-11-14T07:00:00Z
Creation Date: 2019-11-14T07:00:00Z
Registrar Registration Expiration Date: 2020-11-14T07:00:00Z
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-92a0cc0348da850269edba8987d20d00@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-92a0cc0348da850269edba8987d20d00@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-92a0cc0348da850269edba8987d20d00@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

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2019.11.17 18:53:27 -03'00'