Alerta de seguridad informática	8FFR20-00208-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	05 de febrero de 2020
Última revisión	05 de febrero 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 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 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

bancoestada[.]site

bancoestada[.]site/imagenes/comun2008/banca-en-linea-personas[.]php?html

actualizate-bancoestado[.]com

Domain bancoestada.site

bancoestada / site / Subdomains

record type	TTL	value		
A	7207	142.93.221.157		
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	64.32.22.100, 168.235.75.52, 45.32.237.128
NS	172800	ns3.dnsowl.com	Zones on DNS server	45.63.106.63, 45.63.5.234, 209.141.39.150
SOA	172800	Mname	ns1.dnsowl.com	
		Rname	hostmaster.dnsowl.com	
		Serial number	1580909772	
		Refresh	7200	
		Retry	1800	
		Expire	1209600	
		Minimum TTL	600	

Domain actualizate-bancoestado.com

actualizate-bancoestado / com / Subdomains

record type	TTL	value		
A	14400	66.45.226.106		
NS	86400	dns2042a.trouble-free.net	Zones on DNS server	173.225.100.50
NS	86400	dns2042b.trouble-free.net	Zones on DNS server	173.225.100.51
MX	14400	0 actualizate-bancoestado.com		
TXT	14400	v=spf1 +a +mx +ip4:173.225.100.50 include:relay.mailchannels.net ~all		
SOA	86400	Mname	dns2042a.trouble-free.net	
		Rname	not-monitored-email.interserver.net	
		Serial number	2020020502	
		Refresh	3600	
		Retry	1800	
		Expire	1209600	
		Minimum TTL	86400	

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

Certificados

Subject DN	CN=www.bancoestada.site
Issuer DN	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
Serial	264846725919976071702274973243578465212737
Validity	2020-02-04 04:43:57 **to** 2020-05-04 04:43:57 (90 days, 0:00:00)
Names	www.bancoestada.site

Subject DN	CN=actualizate-bancoestado.com
Issuer DN	C=US, ST=TX, L=Houston, O=cPanel, Inc., CN=cPanel, Inc. Certification Authority
Serial	101651782660243945867646781400582933054
Validity	2020-02-05 00:00:00 **to** 2020-05-05 23:59:59 (90 days, 23:59:59)
Names	actualizate-bancoestado.com cpanel.actualizate-bancoestado.com mail.actualizate-bancoestado.com mail.wh477734.ispot.cc webdisk.actualizate-bancoestado.com webmail.actualizate-bancoestado.com wh477734.ispot.cc www.actualizate-bancoestado.com www.wh477734.ispot.cc

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

IP

142[.]93[.]221[.]157

66[.]45[.]226[.]106

Domain bancoestada.site is located on IP address << 142.93.221.157 >>

Block start	142.93.0.0
End of block	142.93.255.255
Block size	65536 Domains in block
Block name	SEARSCANADA-93
AS number	14061
Parent block	142.0.0.0 - 142.255.255.255
Organization	Sears Canada Inc.
City	NORTH YORK
Region/State	Ontario
Country	CA , Canada
Reg. date	1991-12-30
Host name	no record in reverse zone

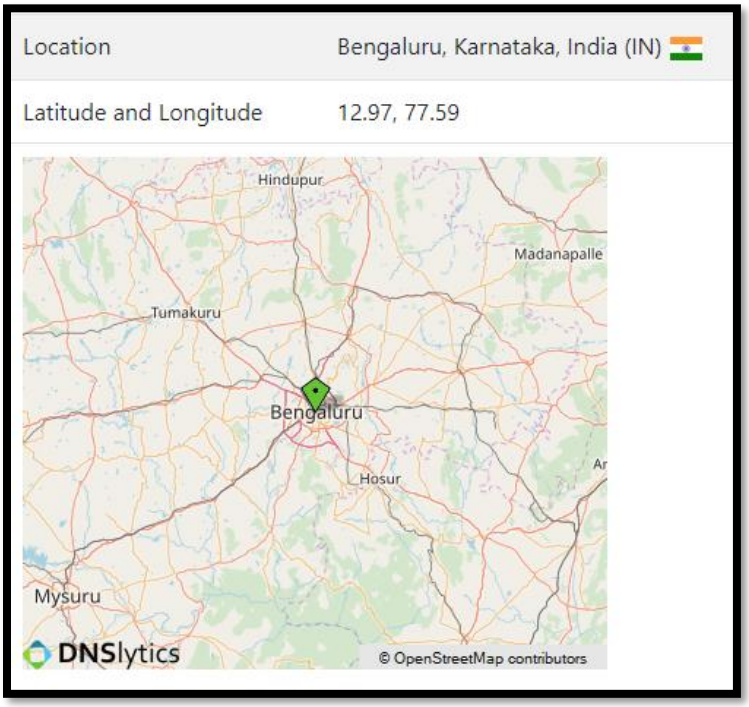
Domain actualizate-bancoestado.com is located on IP address << 66.45.226.106 >>

Block start	66.45.224.0
End of block	66.45.255.255
Block size	8192 Domains in block
Block name	INTERSERVER
AS number	19318
Parent block	66.0.0.0 - 66.255.255.255
Organization	Interserver, Inc
City	Secaucus
Region/State	New Jersey
Country	US , United States
Reg. date	2003-09-23
Host name	unixserver7.unixsrv7.com
Web server	Apache/2.2.26 (Unix) mod_ssl/2.2.26 OpenSSL/0.9.8e-fips-rhel5 mod_auth_passthrough/2.1 mod_bwlimited/1.4 FrontPage/5.0.2.2635 PHP/5.3.27

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

Localización

India, Bangalore, Karnataka



USA, Secaucus, New Jersey

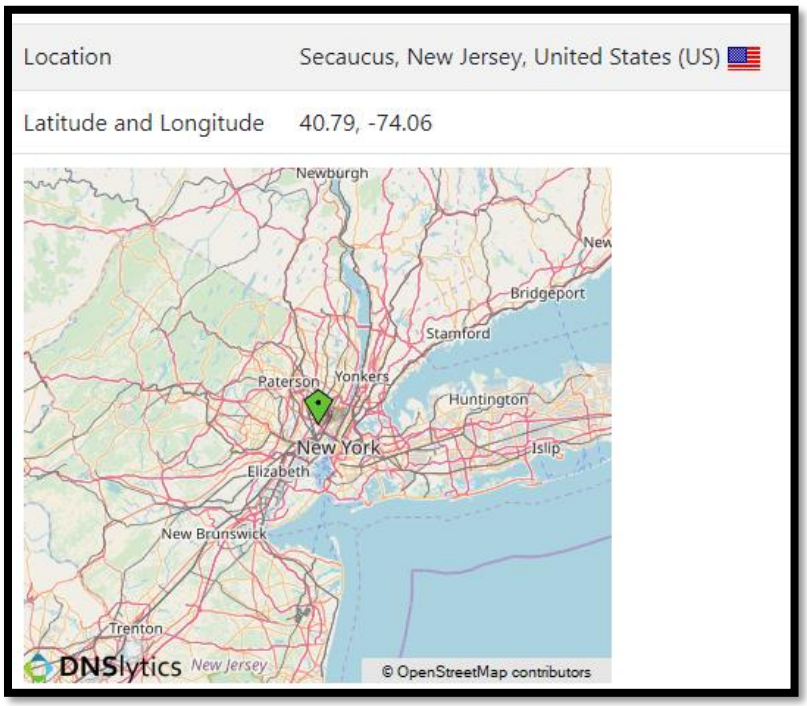
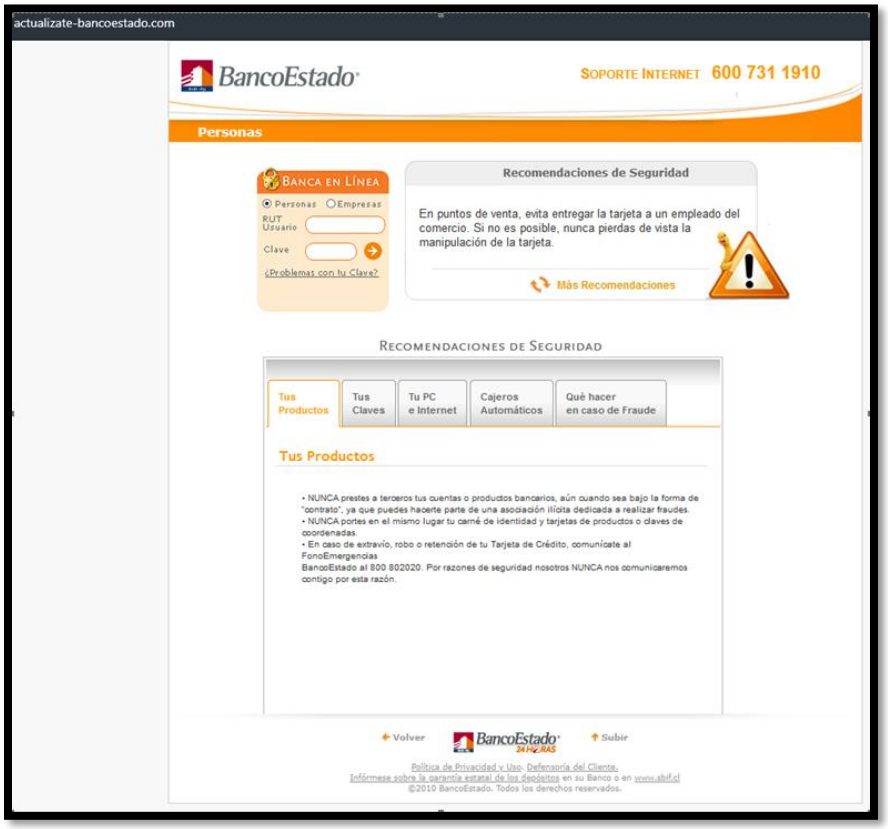


Imagen del sitio



Whois

```
Domain Name: bancoestada.site
Registry Domain ID: D169441996-CNIC
Registrar WHOIS Server: whois.namesilo.com
Registrar URL: https://www.namesilo.com/
Updated Date: 2020-02-04T07:00:00Z
Creation Date: 2020-02-03T07:00:00Z
Registrar Registration Expiration Date: 2021-02-04T07:00:00Z
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-7adf1b4e755b55a8ad20388d486e97a7@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-7adf1b4e755b55a8ad20388d486e97a7@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-7adf1b4e755b55a8ad20388d486e97a7@privacyguardian.org
Name Server: NS1.DNSOWL.COM
Name Server: NS2.DNSOWL.COM
Name Server: NS3.DNSOWL.COM
DNSSEC: unsigned
```

```
whois -I  bancoestado.com
% IANA WHOIS server
% for more information on IANA, visit http://www.iana.org
% This query returned 1 object

refer:        whois.verisign-grs.com

domain:       COM

organisation: VeriSign Global Registry Services
address:      12061 Bluemont Way
address:      Reston Virginia 20190
address:      United States

contact:      administrative
name:         Registry Customer Service
organisation: VeriSign Global Registry Services
address:      12061 Bluemont Way
address:      Reston Virginia 20190
address:      United States
phone:        +1 703 925-6999
fax-no:       +1 703 948 3978
e-mail:       info@verisign-grs.com

contact:      technical
name:         Registry Customer Service
organisation: VeriSign Global Registry Services
address:      12061 Bluemont Way
address:      Reston Virginia 20190
address:      United States
phone:        +1 703 925-6999
fax-no:       +1 703 948 3978
e-mail:       info@verisign-grs.com

nserver:      A.GTLD-SERVERS.NET 192.5.6.30 2001:503:a83e:0:0:0:2:30
nserver:      B.GTLD-SERVERS.NET 192.33.14.30 2001:503:231d:0:0:0:2:30
nserver:      C.GTLD-SERVERS.NET 192.26.92.30 2001:503:83eb:0:0:0:0:30
nserver:      D.GTLD-SERVERS.NET 192.31.80.30 2001:500:856e:0:0:0:0:30
nserver:      E.GTLD-SERVERS.NET 192.12.94.30 2001:502:1ca1:0:0:0:0:30
nserver:      F.GTLD-SERVERS.NET 192.35.51.30 2001:503:d414:0:0:0:0:30
nserver:      G.GTLD-SERVERS.NET 192.42.93.30 2001:503:eea3:0:0:0:0:30
nserver:      H.GTLD-SERVERS.NET 192.54.112.30 2001:502:8cc:0:0:0:0:30
nserver:      I.GTLD-SERVERS.NET 192.43.172.30 2001:503:39c1:0:0:0:0:30
nserver:      J.GTLD-SERVERS.NET 192.48.79.30 2001:502:7094:0:0:0:0:30
nserver:      K.GTLD-SERVERS.NET 192.52.178.30 2001:503:d2d:0:0:0:0:30
nserver:      L.GTLD-SERVERS.NET 192.41.162.30 2001:500:d937:0:0:0:0:30
nserver:      M.GTLD-SERVERS.NET 192.55.83.30 2001:501:b1f9:0:0:0:0:30
ds-rdata:     30909 8 2 E2D3C916F6DEEAC73294E8268FB5885044A833FC5459588F4A9184CFC41A5766

whois:        whois.verisign-grs.com

status:       ACTIVE
remarks:      Registration information: http://www.verisigninc.com

created:      1985-01-01
changed:      2017-10-05
source:       IANA

   Domain Name: BANCOESTADO.COM
   Registry Domain ID: 9950946_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.godaddy.com
   Registrar URL: http://www.godaddy.com
```

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: 2020.02.06 09:37:43 -03'00'