Alerta de seguridad informática	**8FFR-00079-001**
Clase de alerta	**Fraude**
Tipo de incidente	**Falsificación de Registros o Identidad**
Nivel de riesgo	**Alto**
TLP	**Blanco**
Fecha de lanzamiento original	**05 de Octubre de 2019**
Última revisión	**05 de Octubre 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 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

www[.]robertjkenner[.]com/tmp_files/Activacion[.]php

http[://]nanara[.]jp/modules/www[.]bancoestado[.]cl/imagenes/comun2008/banca-en-linea-personas[.]html

https[://]www[.]bancoestadocll[.]xyz

Domain nanara.jp

nanara / jp / Subdomains

record type	TTL	value		
A	10800	160.153.129.229		
NS	3600	ns41.domaincontrol.com	Zones on DNS server	97.74.100.21
NS	3600	ns42.domaincontrol.com	Zones on DNS server	173.201.68.21
SOA	3600	Mname	ns41.domaincontrol.com	
		Rname	dns.jomax.net	
		Serial number	2019091600	
		Refresh	28800	
		Retry	7200	
		Expire	604800	
		Minimum TTL	600	

Domain www.bancoestadocll.xyz

www / bancoestadocll / xyz / Subdomains

record type	TTL	value
A	7207	165.22.216.74

Ilustración 1 Dominio donde se Aloja Url del Banco Estado, Falso

IP´s

160[.]153[.]129[.]229

165[.]22[.]216[.]74

Domain nanara.jp is located on IP address << 160.153.129.229 >>	
Block start	160.153.0.0
End of block	160.153.255.255
Block size	65536 Domains in block
Block name	GO-DADDY-COM-LLC
AS number	26496
Parent block	160.0.0.0 - 160.255.255.255
Organization	GoDaddy.com, LLC
City	Scottsdale
Region/State	Arizona
Country	US , United States
Reg. date	2011-09-01
Host name	ip-160-153-129-229.ip.secureserver.net
Web server	Apache/2.4.23

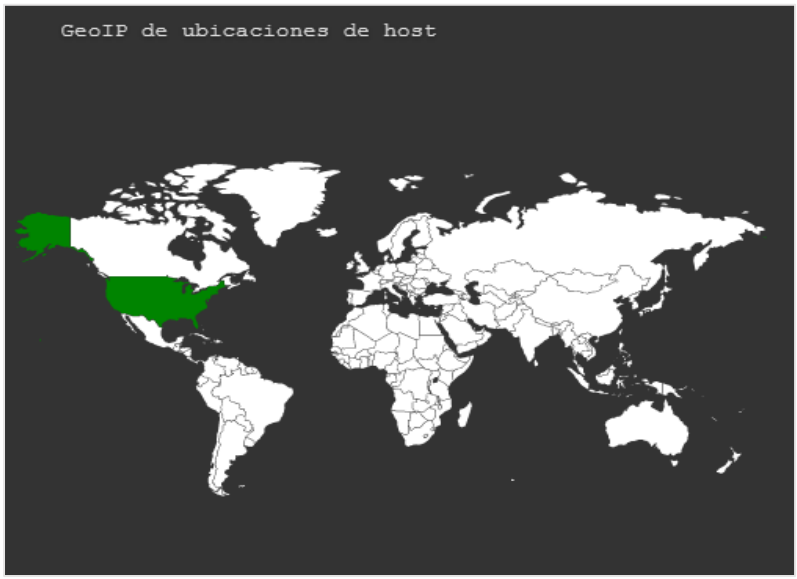
Domain www.bancoestadocll.xyz is located on IP address << 165.22.216.74 >>	
Block start	165.22.0.0
End of block	165.22.255.255
Block size	65536 Domains in block
Block name	CELTECH1
AS number	14061
Parent block	165.0.0.0 - 165.255.255.255
Organization	CellularTechnicalServices
City	Seattle
Region/State	Washington
Country	US , United States
Reg. date	1993-03-31
Host name	no record in reverse zone
Domains	1 www.bancoestadocll.xyz

Ilustración 2 Ip de Origen donde se aloja Sitio Falso del Banco Estado

Localización

Scottsdale, Arizona, Estados Unidos

Seattle, Estados Unidos



www.bancoestadocll.xyz 165.22.216.74

United States

SSH: SSH-2.0-OpenSSH_7.2p2 Ubuntu-4ubuntu2.8

Certificados

Certificates

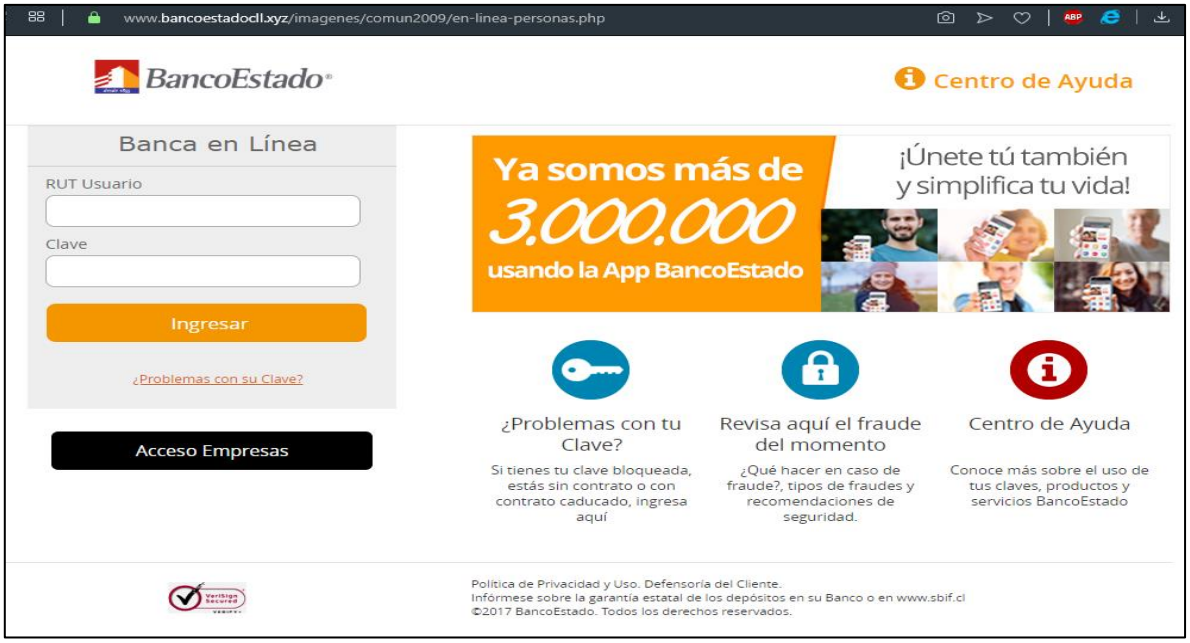
crt.sh ID	Logged At ⇧	Not Before	Not After	Issuer Name
1957791393	2019-10-04	2019-10-04	2020-01-02	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1957451158	2019-10-04	2019-10-04	2020-01-02	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3

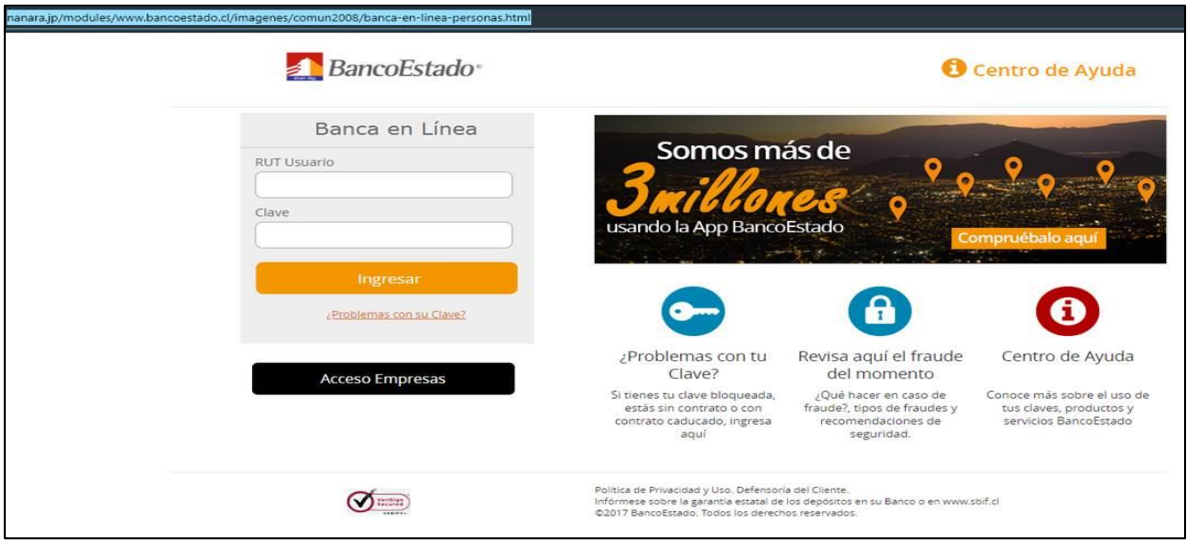
Certificates

crt.sh ID	Logged At ⇧	Not Before	Not After	Issuer Name
69934068	2016-12-22	2016-12-15	2017-03-15	C=US, ST=TX, L=Houston, O="cPanel, Inc.", CN="cPanel, Inc. Certification Authority"

Ilustración 3 Certificado Utilizado en Url del sitio Falso del Banco Estado

Imagen del sitio





Whois

```
soc@misp:~$ whois nanara.jp
[ JPRS database provides information on network administration. Its use is    ]
[ restricted to network administration purposes. For further information,     ]
[ use 'whois -h whois.jprs.jp help'. To suppress Japanese output, add'/e'     ]
[ at the end of command, e.g. 'whois -h whois.jprs.jp xxx/e'.                 ]

Domain Information:
[Domain Name]                   NANARA.JP

[Registrant]                    Naomura Planning co.,ltd

[Name Server]                   ns41.domaincontrol.com
[Name Server]                   ns42.domaincontrol.com
[Signing Key]

[Created on]                    2016/03/12
[Expires on]                    2020/03/31
[Status]                        Active
[Last Updated]                  2019/04/01 01:12:57 (JST)

Contact Information:
[Name]                          Whois Privacy Protection Service by onamae.com
[Email]                         proxy@whoisprotectservice.com
[Web Page]
[Postal code]                   150-8512
[Postal Address]                Shibuya-ku
                                26-1 Sakuragaoka-cho
                                Cerulean Tower 11F
[Phone]                         +81.354562560
[Fax]
```

```
soc@misp:~$ whois -h whois.namesilo.com bancoestadocll.xyz
Domain Name: bancoestadocll.xyz
Registrar WHOIS Server: whois.namesilo.com
Registrar URL: https://www.namesilo.com/
Updated Date: 2019-10-04T07:00:00Z
Creation Date: 2019-10-04T07:00:00Z
Registrar Registration Expiration Date: 2020-10-04T07:00:00Z
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-cd96dba0c7175d375d8ff372716115ba@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-cd96dba0c7175d375d8ff372716115ba@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-cd96dba0c7175d375d8ff372716115ba@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: 2019-10-04T07:00:00Z <<<

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
Data in our WHOIS database is provided for information purposes only, and to
```

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: 2019.10.05 11:10:41 -03'00'