| | |
|---|---|
| **Alerta de seguridad informática** | **8FFR-00078-001** |
| **Clase de alerta** | **Fraude** |
| **Tipo de incidente** | **Falsificación de Registros o Identidad** |
| **Nivel de riesgo** | **Alto** |
| **TLP** | **Blanco** |
| **Fecha de lanzamiento original** | **03 de Octubre de 2019** |
| **Última revisión** | **03 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

https[://]bancoestado[.]cc/

**Domain bancoestado.cc**

bancoestado / cc / Subdomains

| record type | TTL | value | | |
|---|---|---|---|---|
| A | 1200 | 198.54.115.179 | | |
| NS | 1800000 | dns1.namecheaphosting.com | Zones on DNS server | 216.87.155.33 |
| NS | 1800000 | dns2.namecheaphosting.com | Zones on DNS server | 216.87.152.33 |
| MX | 1200 | 10 smx1.web-hosting.com | | 162.255.118.61, 162.255.118.62 |
| MX | 1200 | 20 smx2.web-hosting.com | | 162.255.118.62, 162.255.118.61 |
| MX | 1200 | 30 smx3.web-hosting.com | | 162.255.118.62, 162.255.118.61 |
| TXT | 1200 | MAltYWlsLmJhbmNvZXN0YWRvLmNjLgo= | | |
| SOA | 1800000 | Mname | dns1.namecheaphosting.com | |
| | | Rname | audit.namecheaphosting.com | |
| | | Serial number | 2019100103 | |
| | | Refresh | 86400 | |
| | | Retry | 7200 | |
| | | Expire | 3600000 | |
| | | Minimum TTL | 86400 | |

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

### Certificado

Certificates

| crt.sh ID | Logged At ⇧ | Not Before | Not After | Issuer Name |
|---|---|---|---|---|
| 1953564373 | 2019-10-03 | 2019-10-03 | 2020-10-02 | C=GB, ST=Greater Manchester, L=Salford, O=Sectigo Limited, CN=Sectigo RSA Domain Validation Secure Server CA |
| 1953564347 | 2019-10-03 | 2019-10-03 | 2020-10-02 | C=GB, ST=Greater Manchester, L=Salford, O=Sectigo Limited, CN=Sectigo RSA Domain Validation Secure Server CA |

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

**IP´s**

198[.]54[.]115[.]179

| Domain bancoestado.cc is located on IP address << 198.54.115.179 >> | |
|---|---|
| **Block start** | 198.54.112.0 |
| **End of block** | 198.54.127.255 |
| **Block size** | 4096 Domains in block |
| **Block name** | ROSS-NET4 |
| **AS number** | 22612 |
| **Parent block** | 198.0.0.0 - 198.255.255.255 |
| **Organization** | Ross Technology Inc. |
| **City** | Atlanta |
| **Region/State** | Georgia |
| **Country** | US , United States |
| **Reg. date** | 2012-07-30 |
| **Host name** | s234.web-hosting.com |
| **Web server** | Apache |
| **Domain count** | >= 262 Servers around |

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

**Localización**

Atlanta, Georgia, Estados Unidos

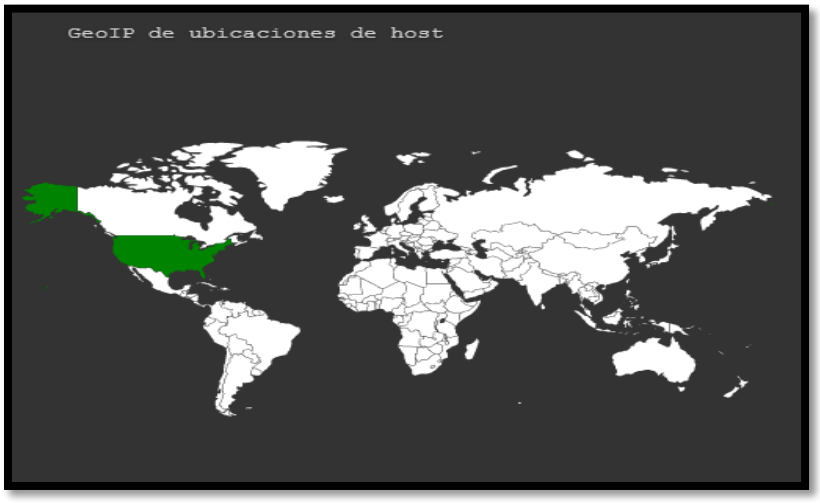
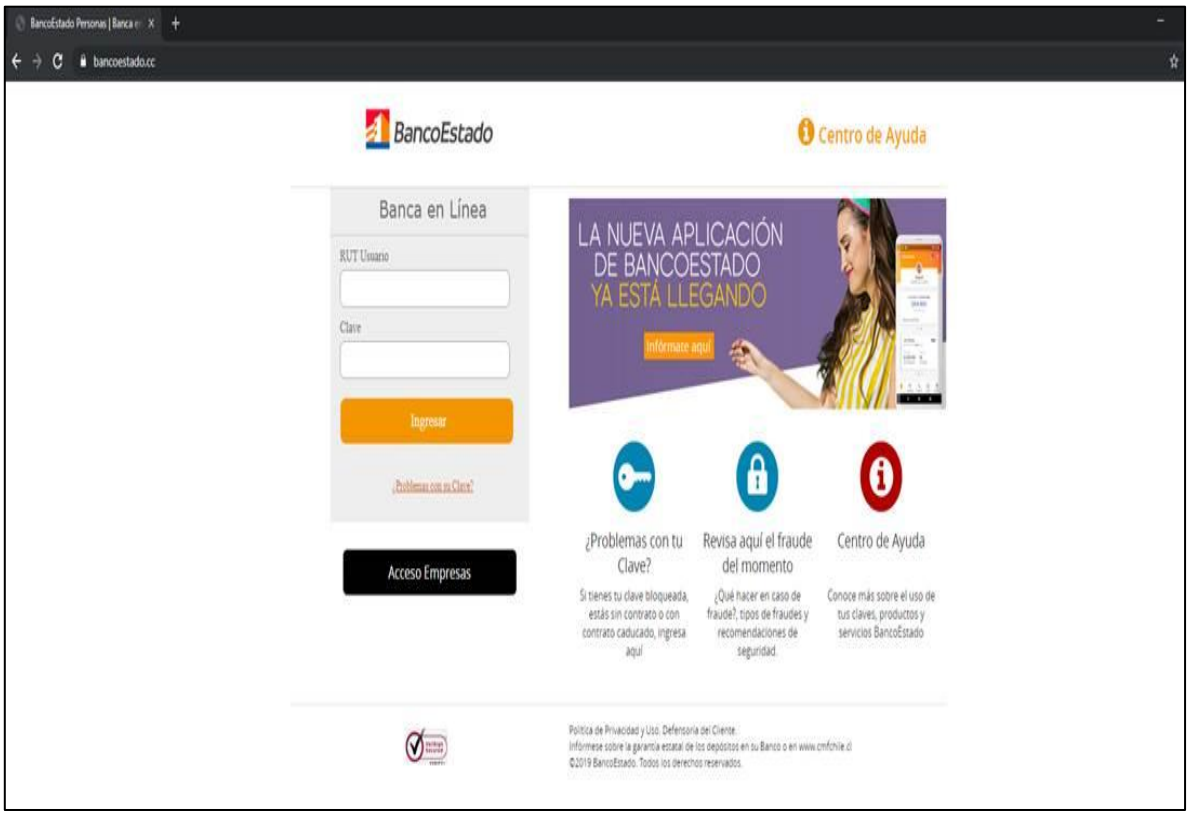


**Imagen del sitio**



## Whois

```
soc@misp:~$ whois -h whois.namecheap.com bancoestado.cc
Domain name: bancoestado.cc
Registry Domain ID: 144737607_DOMAIN_CC-VRSN
Registrar WHOIS Server: whois.namecheap.com
Registrar URL: http://www.namecheap.com
Updated Date: 0001-01-01T00:00:00.00Z
Creation Date: 2019-10-01T13:14:19.00Z
Registrar Registration Expiration Date: 2020-10-01T13:14:19.00Z
Registrar: NAMECHEAP INC
Registrar IANA ID: 1068
Registrar Abuse Contact Email: abuse@namecheap.com
Registrar Abuse Contact Phone: +1.6613102107
Reseller: NAMECHEAP INC
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: addPeriod https://icann.org/epp#addPeriod
Registry Registrant ID:
Registrant Name: WhoisGuard Protected
Registrant Organization: WhoisGuard, Inc.
Registrant Street: P.O. Box 0823-03411
Registrant City: Panama
Registrant State/Province: Panama
Registrant Postal Code:
Registrant Country: PA
Registrant Phone: +507.8365503
Registrant Phone Ext:
Registrant Fax: +51.17057182
Registrant Fax Ext:
Registrant Email: 1f3acb9e258b4311a2cfd3cd6b4d9bc8.protect@whoisguard.com
Registry Admin ID:
Admin Name: WhoisGuard Protected
Admin Organization: WhoisGuard, Inc.
Admin Street: P.O. Box 0823-03411
Admin City: Panama
Admin State/Province: Panama
Admin Postal Code:
Admin Country: PA
Admin Phone: +507.8365503
Admin Phone Ext:
Admin Fax: +51.17057182
Admin Fax Ext:
Admin Email: 1f3acb9e258b4311a2cfd3cd6b4d9bc8.protect@whoisguard.com
Registry Tech ID:
Tech Name: WhoisGuard Protected
Tech Organization: WhoisGuard, Inc.
Tech Street: P.O. Box 0823-03411
Tech City: Panama
Tech State/Province: Panama
Tech Postal Code:
Tech Country: PA
Tech Phone: +507.8365503
Tech Phone Ext:
Tech Fax: +51.17057182
Tech Fax Ext:
Tech Email: 1f3acb9e258b4311a2cfd3cd6b4d9bc8.protect@whoisguard.com
Name Server: dns1.namecheaphosting.com
Name Server: dns2.namecheaphosting.com
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2019-10-03T01:12:19.03Z <<<

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

**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: 2019.10.03 15:57:10 -03'00'