Alerta de seguridad informática	8FFR-00170-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	25 de diciembre de 2019
Última revisión	25 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 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[://]www[.]banca-estado[.]xyz/imagenes/comun2008/banca-en-linea-personas[.]php?html

Domain www.banca-estado.xyz

www / banca-estado / xyz / Subdomains

record type	TTL	value
A	7207	206.189.133.61

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

Certificados

Subject DN	CN=www.banca-estado.xyz
Issuer DN	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
Serial	265824625148376093383552142607600188020280
Validity	2019-12-24 08:06:06 **to** 2020-03-23 08:06:06 (90 days, 0:00:00)
Names	www.banca-estado.xyz

Ilustración 2 Certificado Utilizado en Url del sitio Falso de BANCO ESTADO

IP

206[.]189[.]133[.]61

Domain www.banca-estado.xyz is located on IP address << 206.189.133.61 >>

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 www.banca-estado.xyz

Ilustración 3 Ip de Origen donde se aloja Sitio Falso de BANCO ESTADO

Localización

Bangalore, Karnataka, india

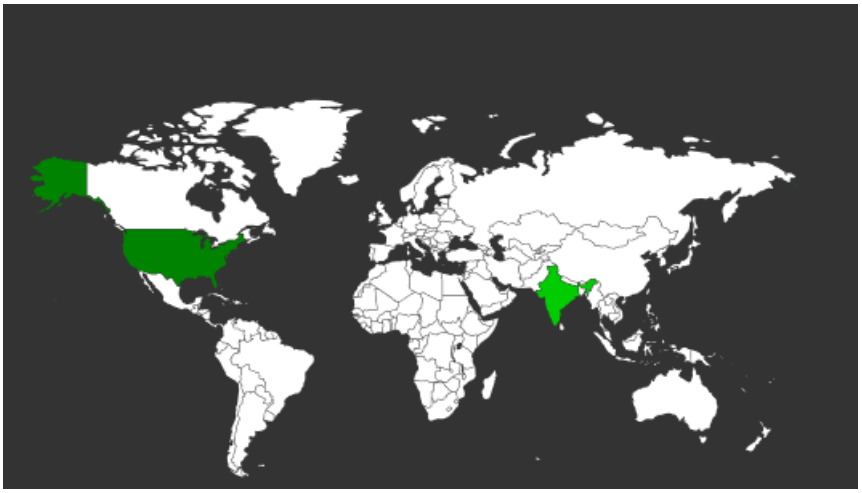

Imagen del sitio

Whois

```
Domain Name: banca-estado.xyz
Registrar WHOIS Server: whois.namesilo.com
Registrar URL: https://www.namesilo.com/
Updated Date: 2019-12-24T07:00:00Z
Creation Date: 2019-12-24T07:00:00Z
Registrar Registration Expiration Date: 2020-12-24T07:00:00Z
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-993ab4bd86c3af632dd46185e9d24ee3@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-993ab4bd86c3af632dd46185e9d24ee3@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-993ab4bd86c3af632dd46185e9d24ee3@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: 2019-12-24T07:00:00Z <<<

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.