Alerta de seguridad informática	8FFR20-00257-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	11 de Marzo de 2020
Última revisión	11 de Marzo 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

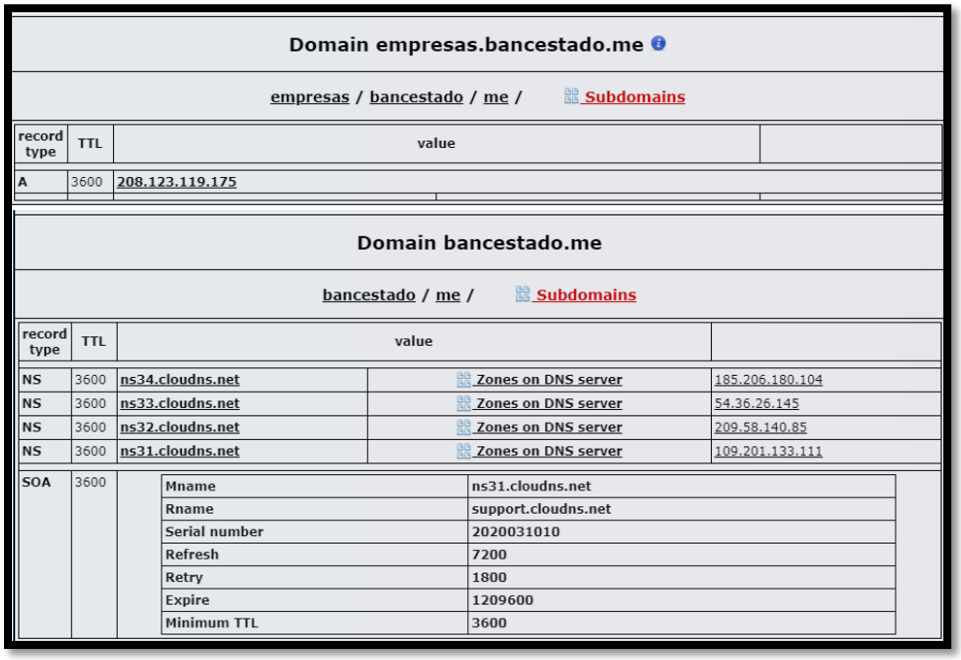
El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de dos portales fraudulentos asociados a una IP que suplantan el sitio web oficial del Banco Estado, el que podría servir para robar credenciales de usuarios de esa entidad.

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

empresas[.]bancestado[.]me
personasestado[.]ddns[.]net



Domain empresas.bancestado.me

empresas / bancestado / me / Subdomains

record type	TTL	value
A	3600	208.123.119.175

Domain bancestado.me

bancestado / me / Subdomains

record type	TTL	value		
NS	3600	ns34.cloudns.net	Zones on DNS server	185.206.180.104
NS	3600	ns33.cloudns.net	Zones on DNS server	54.36.26.145
NS	3600	ns32.cloudns.net	Zones on DNS server	209.58.140.85
NS	3600	ns31.cloudns.net	Zones on DNS server	109.201.133.111

SOA	3600		
		Mname	ns31.cloudns.net
		Rname	support.cloudns.net
		Serial number	2020031010
		Refresh	7200
		Retry	1800
		Expire	1209600
		Minimum TTL	3600

Domain personasestado.ddns.net

personasestado / ddns / net / Subdomains

record type	TTL	value
A	60	208.123.119.175

Domain ddns.net

ddns / net / Subdomains

record type	TTL	value		
A	60	8.23.224.108		
NS	86400	nf1.no-ip.com	Zones on DNS server	194.62.182.53
NS	86400	nf2.no-ip.com	Zones on DNS server	45.54.64.53
NS	86400	nf3.no-ip.com	Zones on DNS server	204.16.253.53
NS	86400	nf4.no-ip.com	Zones on DNS server	194.62.183.53
NS	86400	nf5.no-ip.com	Zones on DNS server	204.16.253.53
MX	1800	5 mail.ddns.net		
SOA	86400	Mname: nf1.no-ip.com Rname: hostmaster.no-ip.com Serial number: 2299124806 Refresh: 10800 Retry: 1800 Expire: 604800 Minimum TTL: 1800		

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

Certificados

Certificates

crt.sh ID	Logged At	Not Before	Not After	Matching Identities	Issuer Name
2562180917	2020-03-10	2020-03-10	2020-06-08	empresas.bancestado.me	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3

Subject DN CN=personasestado.ddns.net

Issuer DN C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3

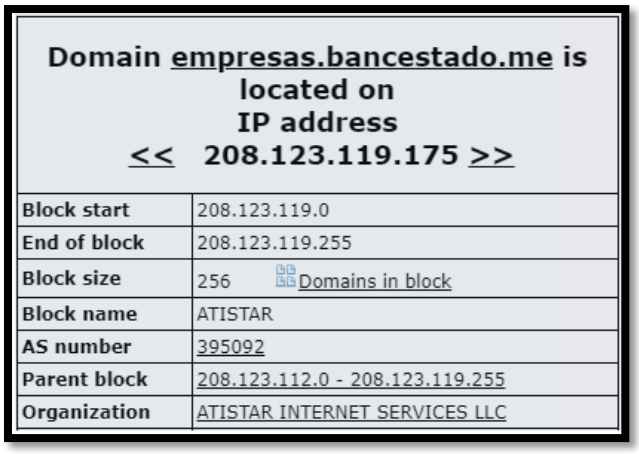
Serial 399024970391864675191502544330318749244790

Validity 2020-03-10 19:51:49 **to** 2020-06-08 19:51:49 (90 days, 0:00:00)

Names personasestado.ddns.net

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

IP
208[.]123[.]119[.]175



Domain empresas.bancestado.me is located on IP address
<< 208.123.119.175 >>

Block start	208.123.119.0
End of block	208.123.119.255
Block size	256 Domains in block
Block name	ATISTAR
AS number	395092
Parent block	208.123.112.0 - 208.123.119.255
Organization	ATISTAR INTERNET SERVICES LLC

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

Localización
Los Ángeles, California, Estados Unidos

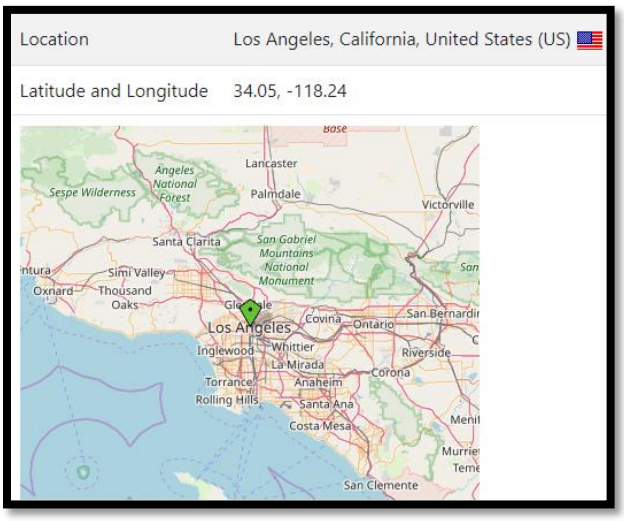
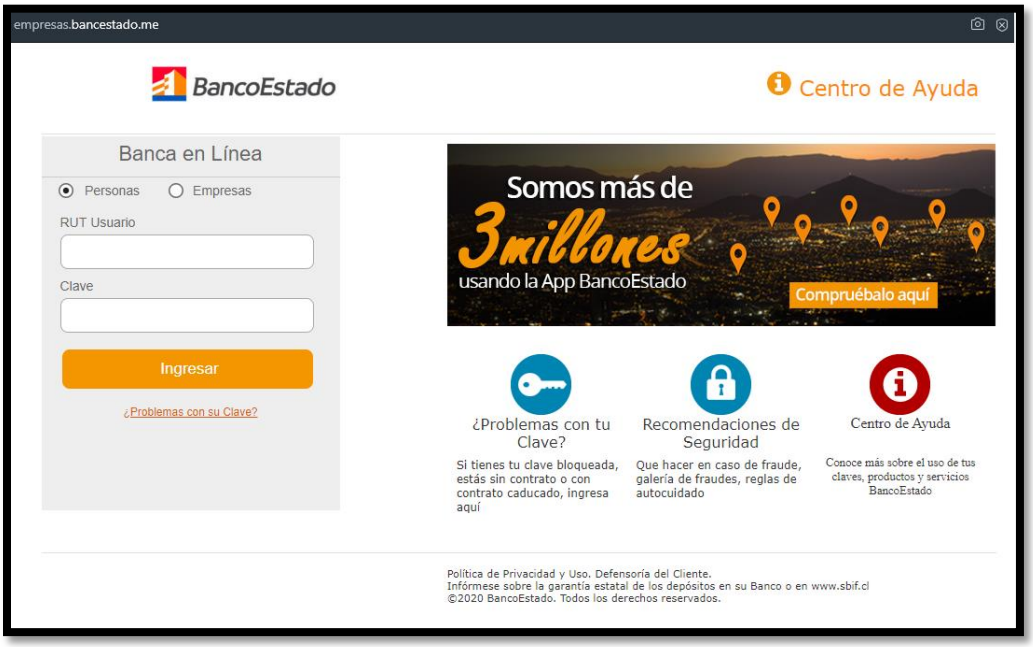
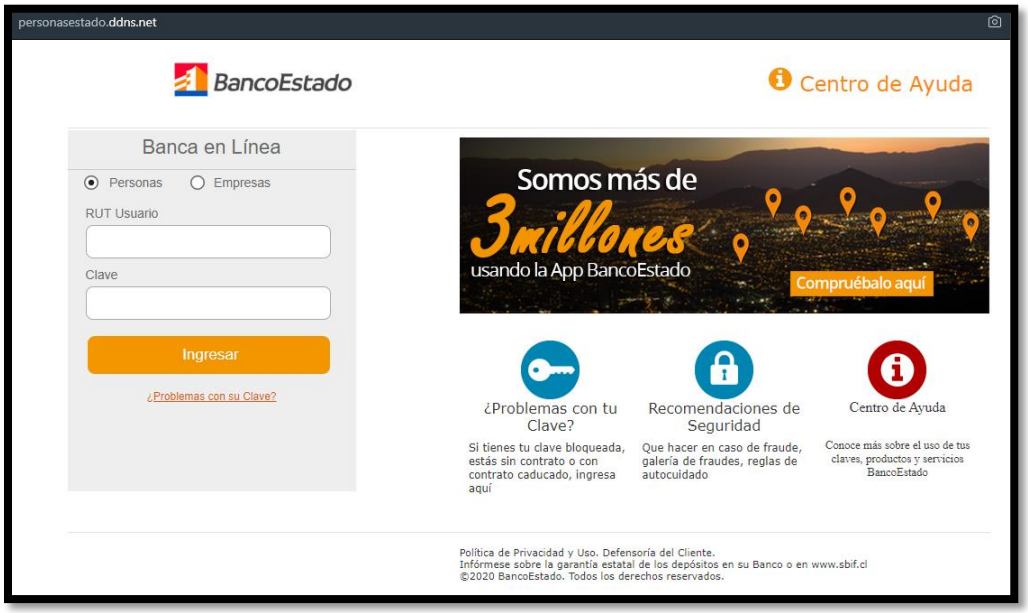


Imagen del sitio





Whois

```
Domain Name: BANCESTADO.ME
Registry Domain ID: D425500000333402249-AGRS
Registrar WHOIS Server: whois.registrar.eu
Registrar URL: www.openprovider.com
Updated Date: 2020-03-10T19:11:28Z
Creation Date: 2020-03-10T13:44:00Z
Registry Expiry Date: 2021-03-10T13:44:00Z
Registrar Registration Expiration Date:
Registrar: Hosting Concepts B.V. d/b/a Openprovider Registrar
Registrar IANA ID: 1647
Registrar Abuse Contact Email: abuse@registrar.eu
Registrar Abuse Contact Phone: +31.104482297
Reseller:
Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
Domain Status: addPeriod https://icann.org/epp#addPeriod
Registrant Organization: Whois Privacy Protection Foundation
Registrant State/Province: Zuid-Holland
Registrant Country: NL
Name Server: NS1.SITE-DNS.COM
Name Server: NS2.SITE-DNS.COM
Name Server: NS3.SITE-DNS.COM
DNSSEC: unsigned
```

```
Domain Name: ddns.net
Registry Domain ID: 73816572_DOMAIN_NET-VRSN
Registrar WHOIS Server: whois.srsplus.com
Registrar URL: http://srsplus.com
Updated Date: 2020-02-07T16:50:29Z
Creation Date: 2001-06-28T16:04:59Z
Registrar Registration Expiration Date: 2022-06-28T16:04:59Z
Registrar: TLDS LLC. d/b/a SRSPlus
Registrar IANA ID: 320
Reseller:
Domain Status: clientTransferProhibited http://icann.org/epp#clientTransferProhibited
Registry Registrant ID:
Registrant Name: Dan Durrer
Registrant Organization: No-IP.com
Registrant Street: 425 Maestro  Dr. Second Floor
Registrant City: Reno
Registrant State/Province: NV
Registrant Postal Code: 89511
Registrant Country: US
Registrant Phone: +1.7758531883
Registrant Phone Ext.:
Registrant Fax:
Registrant Fax Ext.:
Registrant Email: domains@no-ip.com
Registry Admin ID:
Admin Name: Dan Durrer
Admin Organization: No-IP.com
Admin Street: 425 Maestro  Dr. Second Floor
Admin City: Reno
Admin State/Province: NV
Admin Postal Code: 89511
Admin Country: US
Admin Phone: +1.7758531883
Admin Phone Ext.:
Admin Fax:
Admin Fax Ext.:
Admin Email: domains@no-ip.com
Registry Tech ID:
Tech Name: Dan Durrer
Tech Organization: No-IP.com
Tech Street: 425 Maestro  Dr. Second Floor
Tech City: Reno
Tech State/Province: NV
Tech Postal Code: 89511
Tech Country: US
Tech Phone: +1.7758531883
Tech Phone Ext.:
Tech Fax:
Tech Fax Ext.:
Tech Email: domains@no-ip.com
Name Server: nf2.no-ip.com
Name Server: nf1.no-ip.com
Name Server: nf4.no-ip.com
Name Server: nf3.no-ip.com
DNSSEC: Unsigned
Registrar Abuse Contact Email: abuse@web.com
Registrar Abuse Contact Phone: +1.8773812449
```

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.