Alerta de seguridad cibernética	8FFR20-00342-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	16 de abril de 2020
Última revisión	16 de abril 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 dos IPs que suplantan 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 COMPROMISO

URL
estadopromocl[.]info
estado[.]mobileacessocl[.]com

IP
159[.]65[.]149[.]158
80[.]211[.]15[.]66

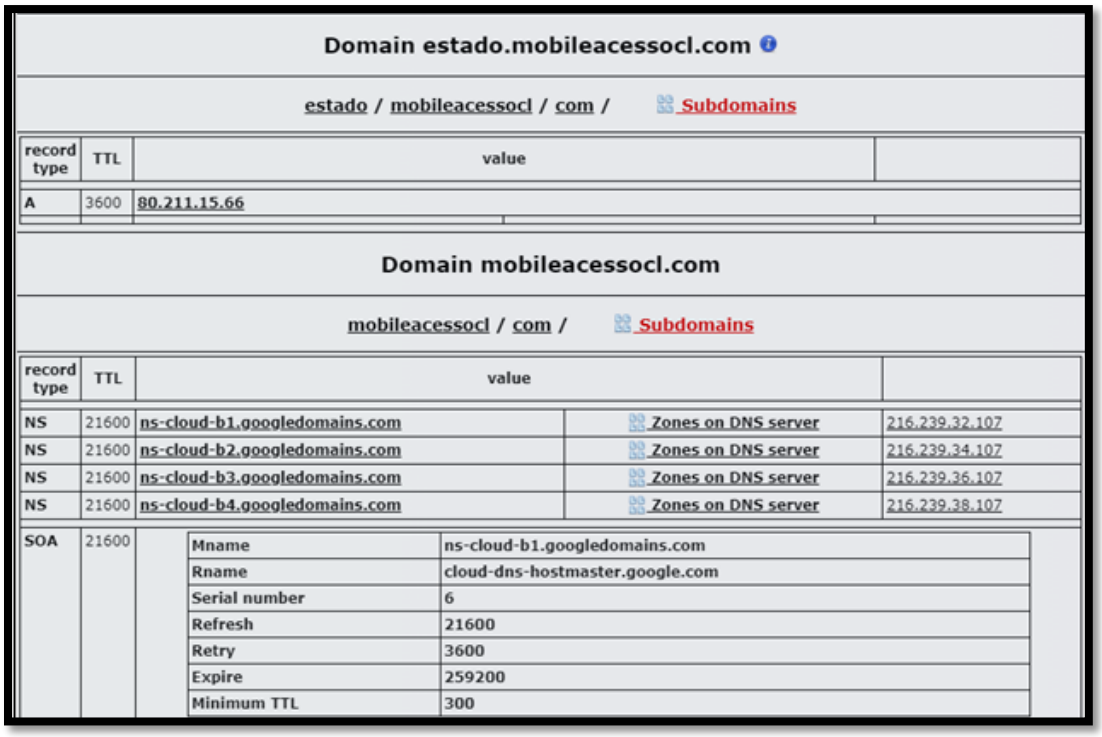
DOMINIOS DONDE SE ALOJA URL

Domain estadopromocl.info

estadopromocl / info / Subdomains

record type	TTL	value		
A	7207	159.65.149.158		
NS	172800	ns1.dnsowl.com	Zones on DNS server	185.34.216.159, 104.207.141.138, 198.251.84.16
NS	172800	ns2.dnsowl.com	Zones on DNS server	168.235.75.52, 45.32.237.128, 64.32.22.100
NS	172800	ns3.dnsowl.com	Zones on DNS server	209.141.39.150, 45.63.5.234, 45.63.106.63

SOA	172800	Mname	ns1.dnsowl.com
		Rname	hostmaster.dnsowl.com
		Serial number	1586967108
		Refresh	7200
		Retry	1800
		Expire	1209600
		Minimum TTL	600



Domain estado.mobileacessocl.com

estado / mobileacessocl / com / Subdomains

record type	TTL	value
A	3600	80.211.15.66

Domain mobileacessocl.com

mobileacessocl / com / Subdomains

record type	TTL	value		
NS	21600	ns-cloud-b1.googledomains.com	Zones on DNS server	216.239.32.107
NS	21600	ns-cloud-b2.googledomains.com	Zones on DNS server	216.239.34.107
NS	21600	ns-cloud-b3.googledomains.com	Zones on DNS server	216.239.36.107
NS	21600	ns-cloud-b4.googledomains.com	Zones on DNS server	216.239.38.107

SOA	21600		
		Mname	ns-cloud-b1.googledomains.com
		Rname	cloud-dns-hostmaster.google.com
		Serial number	6
		Refresh	21600
		Retry	3600
		Expire	259200
		Minimum TTL	300

CERTIFICADOS

Subject DN	CN=estadopromocl.info
Issuer DN	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
Serial	405301330362074957708715175530267194995050
Validity	2020-04-15 05:11:30 **to** 2020-07-14 05:11:30 (90 days, 0:00:00)
Names	estadopromocl.info

Subject DN	CN=estado.mobileacessocl.com
Issuer DN	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
Serial	265864055896546542338181186481275223838954
Validity	2020-04-15 09:28:42 **to** 2020-07-14 09:28:42 (90 days, 0:00:00)
Names	estado.mobileacessocl.com

IP DE ORIGEN DONDE SE ALOJA SITIO

Domain estadopromocl.info is located on IP address << 159.65.149.158 >>

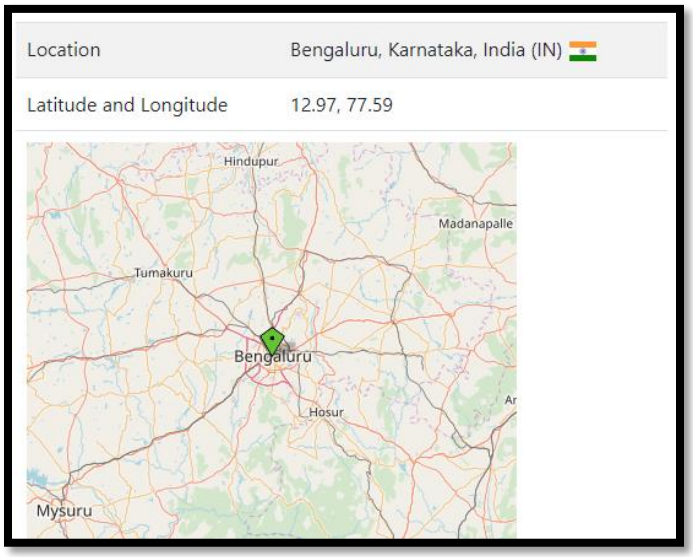
Block start	159.65.0.0
End of block	159.65.255.255
Block size	65536 Domains in block
Block name	PHS-NET
AS number	14061
Parent block	159.0.0.0 - 159.255.255.255
Organization	PresbyterianHealthcareSys.

Domain estado.mobileacessocl.com is located on IP address << 80.211.15.66 >>

Block start	80.211.15.0
End of block	80.211.15.255
Block size	256 Domains in block
Block name	ARUBA-NET
AS number	31034
Parent block	80.211.0.0 - 80.211.127.255
Organization	Aruba S.p.A. - Cloud Services Farm2

LOCALIZACIÓN

Bengaluru, Karnataka, India



Arezzo, Tuscany, Italia

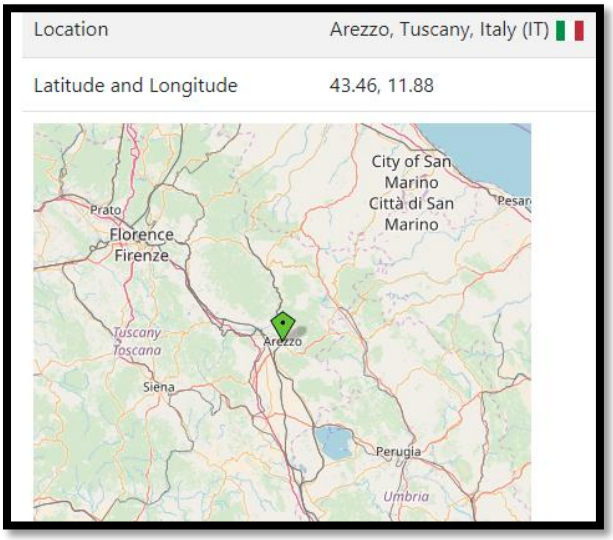
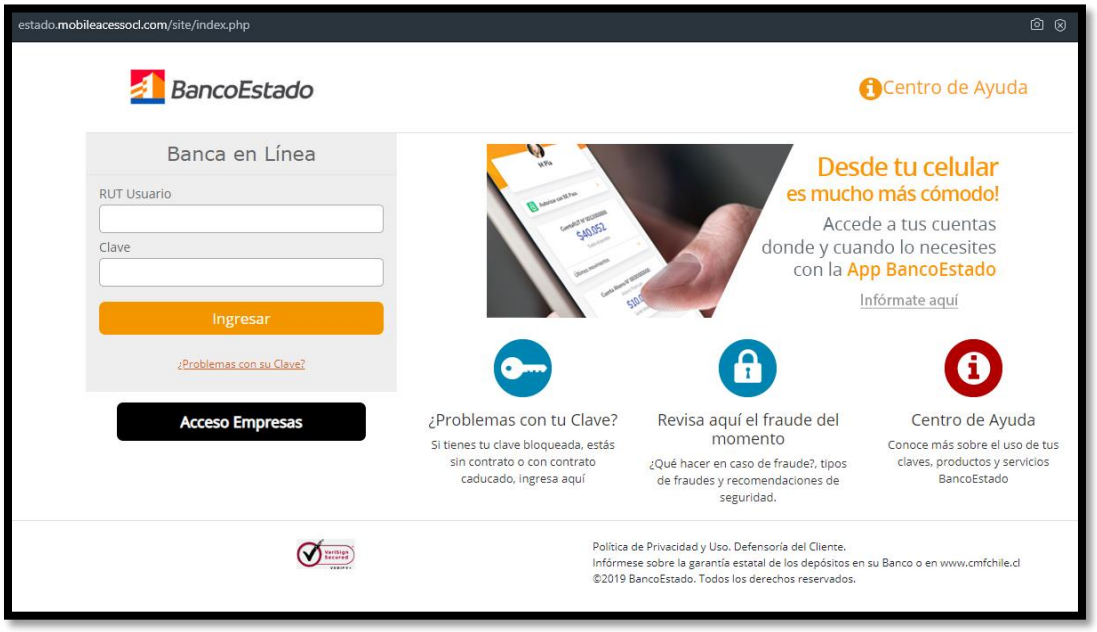


IMAGEN DEL SITIO



WHOIS

```
Domain Name: mobileacessocl.com
Registry Domain ID: 2514927413_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.google.com
Registrar URL: https://domains.google.com
Updated Date: 2020-04-15T08:54:04Z
Creation Date: 2020-04-15T08:54:03Z
Registrar Registration Expiration Date: 2021-04-15T08:54:03Z
Registrar: Google LLC
Registrar IANA ID: 895
Registrar Abuse Contact Email: registrar-abuse@google.com
Registrar Abuse Contact Phone: +1.8772376466
Domain Status: clientTransferProhibited https://www.icann.org/epp#clientTransferProhibited
Registry Registrant ID:
Registrant Name: Contact Privacy Inc. Customer 1246942212
Registrant Organization: Contact Privacy Inc. Customer 1246942212
Registrant Street: 96 Mowat Ave
Registrant City: Toronto
Registrant State/Province: ON
Registrant Postal Code: M4K 3K1
Registrant Country: CA
Registrant Phone: +1.4165385487
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: k98gkt6imkgk@contactprivacy.email
Registry Admin ID:
Admin Name: Contact Privacy Inc. Customer 1246942212
Admin Organization: Contact Privacy Inc. Customer 1246942212
Admin Street: 96 Mowat Ave
Admin City: Toronto
Admin State/Province: ON
Admin Postal Code: M4K 3K1
Admin Country: CA
Admin Phone: +1.4165385487
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: k98gkt6imkgk@contactprivacy.email
Registry Tech ID:
Tech Name: Contact Privacy Inc. Customer 1246942212
Tech Organization: Contact Privacy Inc. Customer 1246942212
Tech Street: 96 Mowat Ave
Tech City: Toronto
Tech State/Province: ON
Tech Postal Code: M4K 3K1
Tech Country: CA
Tech Phone: +1.4165385487
Tech Phone Ext:
Tech Fax:
Tech Fax Ext:
Tech Email: k98gkt6imkgk@contactprivacy.email
Name Server: NS-CLOUD-B1.GOOGLEDOMAINS.COM
Name Server: NS-CLOUD-B2.GOOGLEDOMAINS.COM
Name Server: NS-CLOUD-B3.GOOGLEDOMAINS.COM
Name Server: NS-CLOUD-B4.GOOGLEDOMAINS.COM
```

```
Domain Name: ESTADOPROMOCL.INFO
Registry Domain ID: D503300001183818438-LRMS
Registrar WHOIS Server: whois.namesilo.com
Registrar URL: http://www.namesilo.com
Updated Date: 2020-04-15T05:45:28Z
Creation Date: 2020-04-15T05:41:24Z
Registry Expiry Date: 2021-04-15T05:41:24Z
Registrar Registration Expiration Date:
Registrar: Namesilo, LLC
Registrar IANA ID: 1479
Registrar Abuse Contact Email: abuse@namesilo.com
Registrar Abuse Contact Phone: +1.4805240066
Reseller:
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
Domain Status: addPeriod https://icann.org/epp#addPeriod
Registrant Organization: See PrivacyGuardian.org
Registrant State/Province: AZ
Registrant Country: US
Name Server: NS3.DNSOWL.COM
Name Server: NS1.DNSOWL.COM
Name Server: NS2.DNSOWL.COM
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form is https://www.icann.org/wicf/
>>> Last update of WHOIS database: 2020-04-15T16:21:35Z <<<
```

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: 2020.04.16 10:40:54 -04'00'