Alerta de seguridad cibernética	8FFR20-00320-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	08 de abril de 2020
Última revisión	08 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
acceso[.]bacoestado[.]win
acceso[.]bacoestado[.]win/inicio
banco[.]estadopromocion[.]com
banco[.]estadopromocion[.]com/site/index[.]php

IP
68[.]183[.]33[.]42
212[.]237[.]63[.]113

DOMINIOS DONDE SE ALOJA URL

Domain acceso.bacoestado.win

acceso / bacoestado / win / Subdomains

record type	TTL	value
A	3600	68.183.33.42

Domain bacoestado.win

bacoestado / win / Subdomains

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

SOA	172800	Mname	ns1.dnsowl.com
		Rname	hostmaster.dnsowl.com
		Serial number	1586271114
		Refresh	7200
		Retry	1800
		Expire	1209600
		Minimum TTL	600

Domain banco.estadopromocion.com

banco / estadopromocion / com / Subdomains

record type	TTL	value
A	3600	212.237.63.113

Domain estadopromocion.com

estadopromocion / com / Subdomains

record type	TTL	value		
NS	21600	ns-cloud-d1.googledomains.com	Zones on DNS server	216.239.32.109
NS	21600	ns-cloud-d2.googledomains.com	Zones on DNS server	216.239.34.109
NS	21600	ns-cloud-d3.googledomains.com	Zones on DNS server	216.239.36.109
NS	21600	ns-cloud-d4.googledomains.com	Zones on DNS server	216.239.38.109

SOA	21600		
		Mname	ns-cloud-d1.googledomains.com
		Rname	cloud-dns-hostmaster.google.com
		Serial number	3
		Refresh	21600
		Retry	3600
		Expire	259200
		Minimum TTL	300

CERTIFICADOS

crt.sh ID	Logged At	Not Before	Not After	Matching Identities	Issuer Name
2677491719	2020-04-07	2020-04-07	2020-07-06	acceso.bacoestado.win	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
2677106927	2020-04-07	2020-04-07	2020-07-06	acceso.bacoestado.win	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3

crt.sh ID	Logged At	Not Before	Not After	Matching Identities	Issuer Name
2676947858	2020-04-07	2020-04-07	2020-07-06	banco.estadopromocion.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
2676806198	2020-04-07	2020-04-07	2020-07-06	banco.estadopromocion.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3

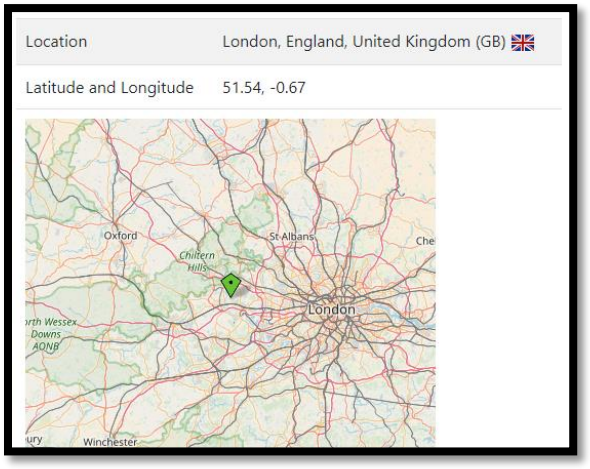
IP DE ORIGEN DONDE SE ALOJA SITIO

Domain acceso.bacoestado.win is located on IP address << 68.183.33.42 >>	
Block start	68.183.0.0
End of block	68.183.255.255
Block size	65536 Domains in block
Block name	DSLEXTREME-NWK-6
AS number	14061
Parent block	68.0.0.0 - 68.255.255.255
Organization	DSL Extreme

Domain banco.estadopromocion.com is located on IP address << 212.237.63.113 >>	
Block start	212.237.63.0
End of block	212.237.63.255
Block size	256 Domains in block
Block name	ARUBA-NET
AS number	31034
Parent block	212.237.0.0 - 212.237.63.255
Organization	Aruba S.p.A. - Cloud Services Farm2

LOCALIZACIÓN

Londres, Inglaterra, Reino Unido



Arezzo, Tuscany, Italia

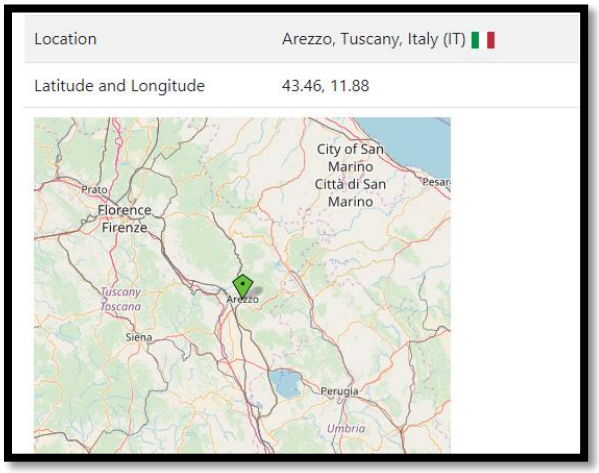
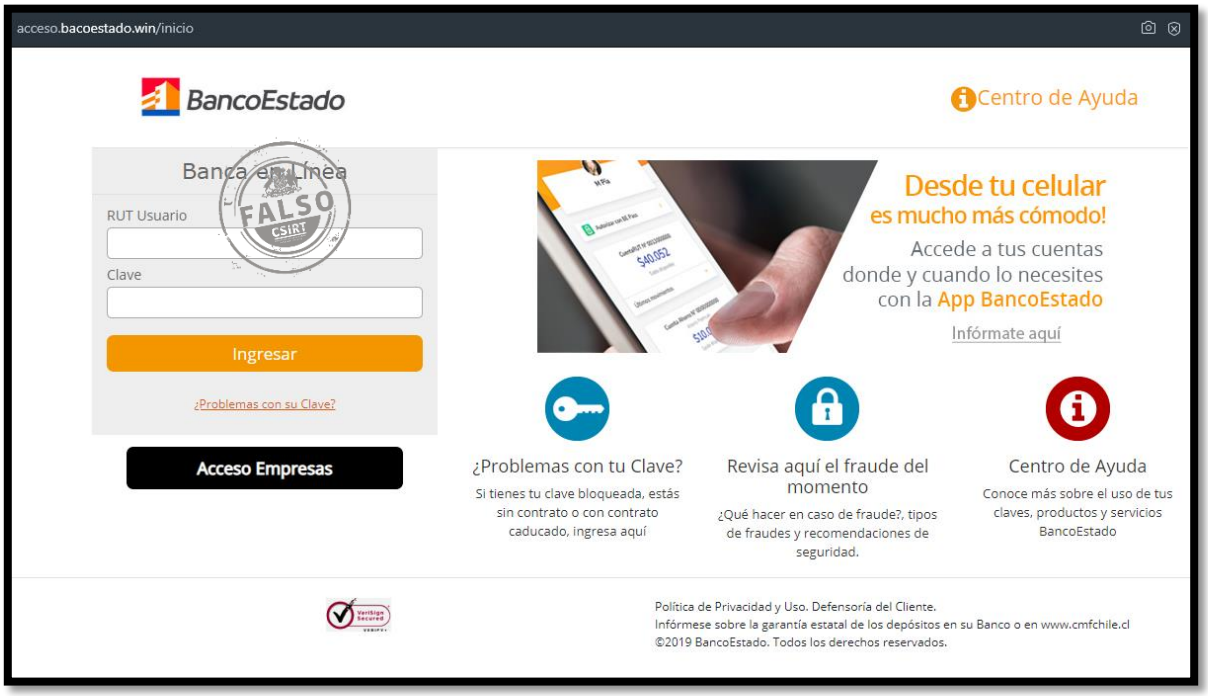
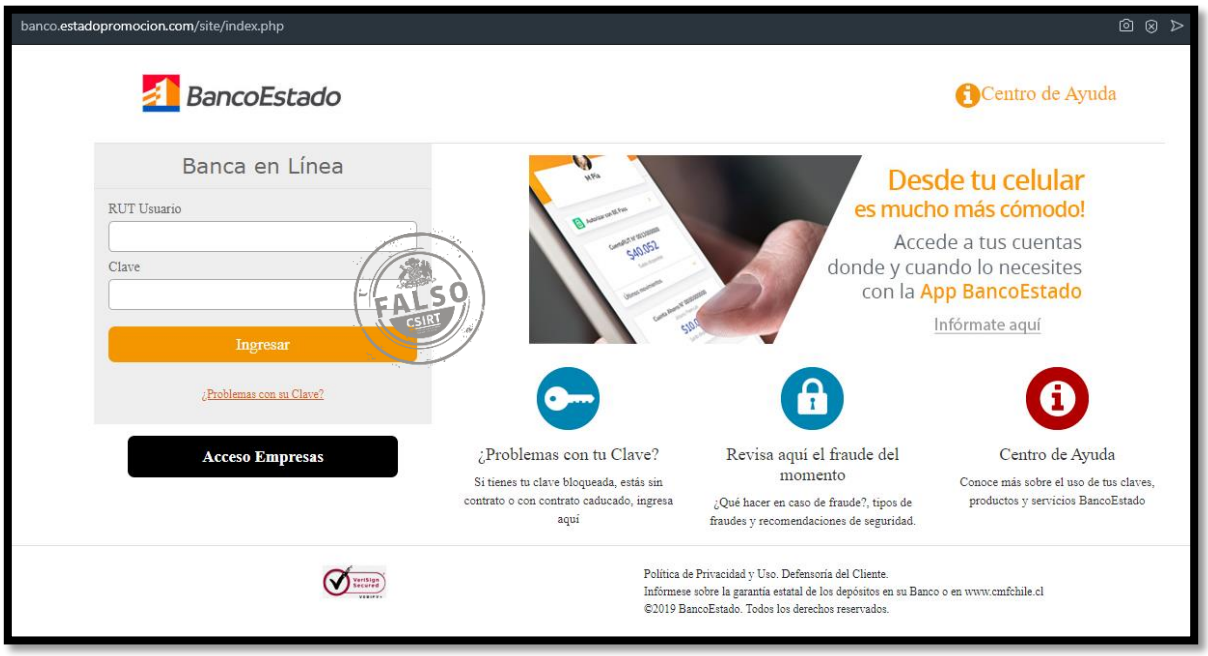


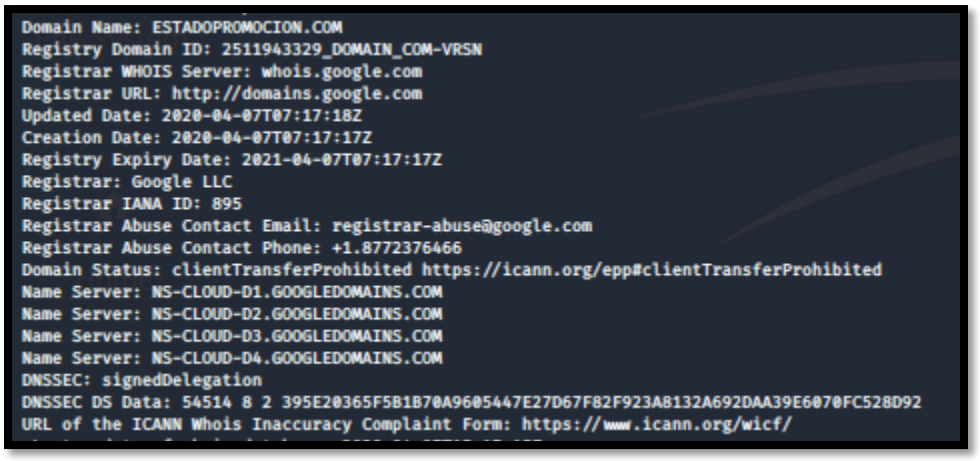
IMAGEN DEL SITIO





WHOIS

```
Domain Name: bacoestado.win
Registry Domain ID: DFA306D155A4349F5B2671D37E389098F-NSR
Registrar WHOIS Server: whois.namesilo.com
Registrar URL: https://www.namesilo.com/
Updated Date: 2020-04-06T07:00:00Z
Creation Date: 2020-04-05T07:00:00Z
Registrar Registration Expiration Date: 2021-04-05T07:00:00Z
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-6f484bc3a833898c3735aa9c9775040e@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-6f484bc3a833898c3735aa9c9775040e@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-6f484bc3a833898c3735aa9c9775040e@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/
```



```
Domain Name: ESTADOPROMOCION.COM
Registry Domain ID: 2511943329_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.google.com
Registrar URL: http://domains.google.com
Updated Date: 2020-04-07T07:17:18Z
Creation Date: 2020-04-07T07:17:17Z
Registry Expiry Date: 2021-04-07T07:17:17Z
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://icann.org/epp#clientTransferProhibited
Name Server: NS-CLOUD-D1.GOOGLEDOMAINS.COM
Name Server: NS-CLOUD-D2.GOOGLEDOMAINS.COM
Name Server: NS-CLOUD-D3.GOOGLEDOMAINS.COM
Name Server: NS-CLOUD-D4.GOOGLEDOMAINS.COM
DNSSEC: signedDelegation
DNSSEC DS Data: 54514 8 2 395E20365F5B1B70A9605447E27D67F82F923A8132A692DAA39E6070FC528D92
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
```

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: 2020.04.08 11:15:26 -04'00'