Alerta de seguridad informática	8FFR20-00272-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	19 de Marzo de 2020
Última revisión	19 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 tres portales fraudulentos asociados a tres IPs que suplantan el sitio web oficial de Banco Estado, el que podrían 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
portal-estado[.]info
portal-estado[.]info/personas/comun2008/banca-en-linea-personas[.]html
portalweb-estado[.]info
portalweb-estado[.]info/personas/comun2008/banca-en-linea-personas[.]html
estado-chile[.]ddns[.]net

Domain portal-estado.info

portal-estado / info / Subdomains

record type	TTL	value		
A	7207	134.122.126.173		
NS	172800	ns1.dnsowl.com	Zones on DNS server	185.34.216.159, 198.251.84.16, 104.207.141.138
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	45.63.106.63, 45.63.5.234, 209.141.39.150
SOA	172800	Mname	ns1.dnsowl.com	
		Rname	hostmaster.dnsowl.com	
		Serial number	1584538629	
		Refresh	7200	
		Retry	1800	
		Expire	1209600	
		Minimum TTL	600	

Domain portalweb-estado.info

portalweb-estado / info / Subdomains

record type	TTL	value		
A	7207	142.93.223.33		
NS	172800	ns1.dnsowl.com	Zones on DNS server	198.251.84.16, 185.34.216.159, 104.207.141.138
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	45.63.106.63, 45.63.5.234, 209.141.39.150
SOA	172800	Mname	ns1.dnsowl.com	
		Rname	hostmaster.dnsowl.com	
		Serial number	1584539486	
		Refresh	7200	
		Retry	1800	
		Expire	1209600	
		Minimum TTL	600	

Domain estado-chile.ddns.net

estado-chile / 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: 2299643093 Refresh: 10800 Retry: 1800 Expire: 604800 Minimum TTL: 1800		

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

Certificados

Certificates

crt.sh ID	Logged At	Not Before	Not After	Matching Identities	Issuer Name
2594819588	2020-03-17	2020-03-17	2020-06-15	portal-estado.info	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
2591544766	2020-03-17	2020-03-17	2020-06-15	portal-estado.info	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3

Certificates

crt.sh ID	Logged At	Not Before	Not After	Matching Identities	Issuer Name
2594936021	2020-03-17	2020-03-17	2020-06-15	portalweb-estado.info	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
2591573997	2020-03-17	2020-03-17	2020-06-15	portalweb-estado.info	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3

Certificates

crt.sh ID	Logged At	Not Before	Not After	Matching Identities	Issuer Name
2597278570	2020-03-18	2020-03-18	2020-06-16	estado-chile.ddns.net	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3

Ilustración 1 Certificado Utilizado en Url del sitio Falso del Banco Estado

IP
134[.]122[.]126[.]173
142[.]93[.]223[.]33
208[.]123[.]119[.]175

Domain portal-estado.info is located on IP address << 134.122.126.173 >>

Block start	134.122.0.0
End of block	134.122.255.255
Block size	65536 Domains in block
Block name	PHOENIX
AS number	14061
Parent block	134.0.0.0 - 134.255.255.255
Organization	Phoenix Technologies Ltd.

Domain portalweb-estado.info is located on IP address << 142.93.223.33 >>

Block start	142.93.0.0
End of block	142.93.255.255
Block size	65536 Domains in block
Block name	SEARSCANADA-93
AS number	14061
Parent block	142.0.0.0 - 142.255.255.255
Organization	Sears Canada Inc.

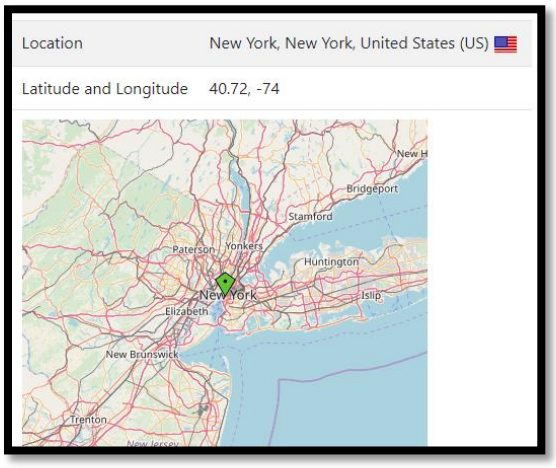
Domain estado-chile.ddns.net is located on IP address << 208.123.119.175 >>

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 1 Ip de Origen donde se aloja Sitio Falso del Banco Estado

Localización

United States of America New York City, New York
Los Angeles, California, United States



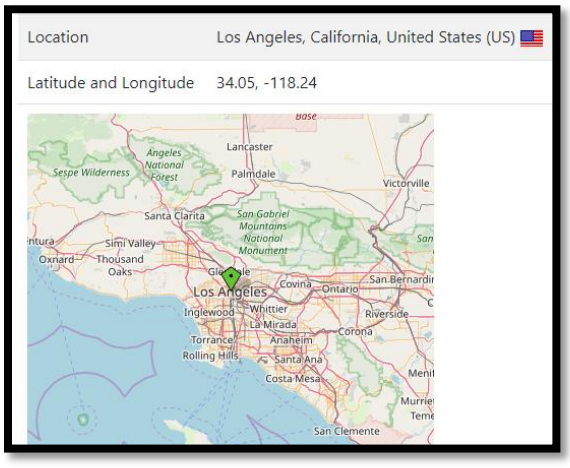
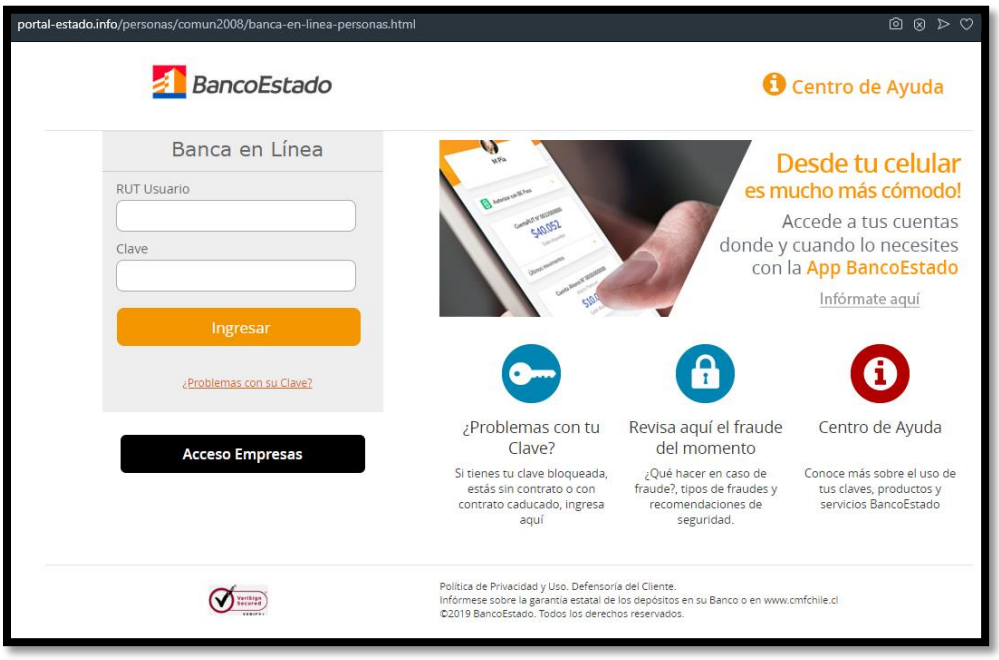
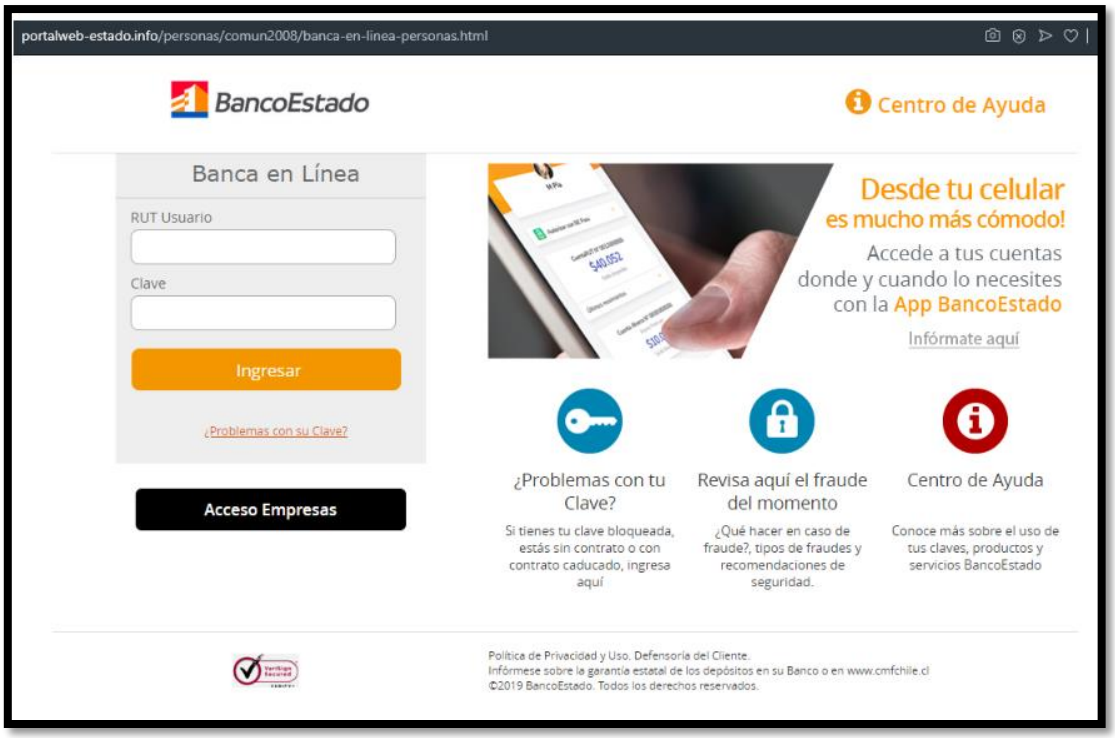
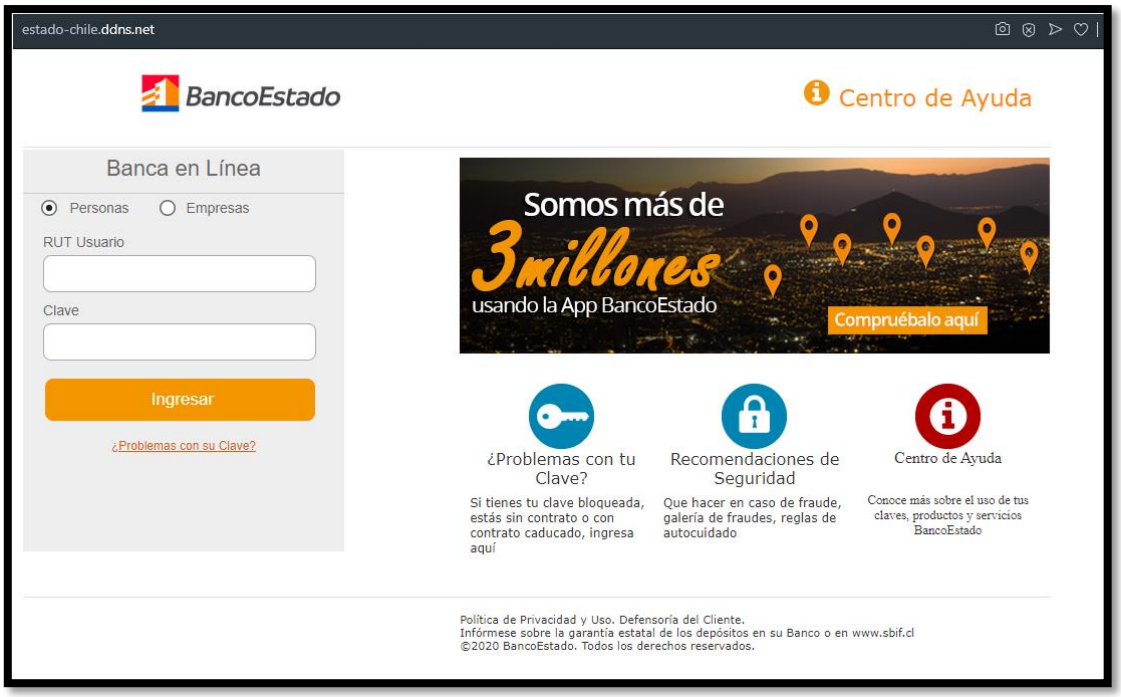


Imagen del sitio




portalweb-estado.info/personas/comun2008/banca-en-linea-personas.html
BancoEstado
Centro de Ayuda
Banca en Línea
RUT Usuario
Clave
Ingresar
¿Problemas con su Clave?
Acceso Empresas
Desde tu celular
es mucho más cómodo!
Accede a tus cuentas
donde y cuando lo necesites
con la App BancoEstado
Infórmate aquí
¿Problemas con tu Clave?
Si tienes tu clave bloqueada, estás sin contrato o con contrato caducado, ingresa aquí
Revisa aquí el fraude del momento
¿Qué hacer en caso de fraude?, tipos de fraudes y recomendaciones de seguridad.
Centro de Ayuda
Conoce más sobre el uso de tus claves, productos y servicios BancoEstado
Política de Privacidad y Uso. Defensoría del Cliente.
Infórmese sobre la garantía estatal de los depósitos en su Banco o en www.cmfchile.cl
©2019 BancoEstado. Todos los derechos reservados.


estado-chile.ddns.net
BancoEstado
Centro de Ayuda
Banca en Línea
Personas
Empresas
RUT Usuario
Clave
Ingresar
¿Problemas con su Clave?
Somos más de
3millones
usando la App BancoEstado
Compruébalo aquí
¿Problemas con tu Clave?
Si tienes tu clave bloqueada, estás sin contrato o con contrato caducado, ingresa aquí
Recomendaciones de Seguridad
Que hacer en caso de fraude, galería de fraudes, reglas de autocuidado
Centro de Ayuda
Conoce más sobre el uso de tus claves, productos y servicios BancoEstado
Política de Privacidad y Uso. Defensoría del Cliente.
Infórmese sobre la garantía estatal de los depósitos en su Banco o en www.sbif.cl
©2020 BancoEstado. Todos los derechos reservados.

Whois

```
Domain Name: PORTAL-ESTADO.INFO
Registry Domain ID: D503300001183549054-LRMS
Registrar WHOIS Server: whois.namesilo.com
Registrar URL: http://www.namesilo.com
Updated Date: 2020-03-17T14:31:14Z
Creation Date: 2020-03-17T14:25:50Z
Registry Expiry Date: 2021-03-17T14:25:50Z
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
```

```
Domain Name: PORTALWEB-ESTADO.INFO
Registry Domain ID: D503300001183549925-LRMS
Registrar WHOIS Server: whois.namesilo.com
Registrar URL: http://www.namesilo.com
Updated Date: 2020-03-17T16:05:02Z
Creation Date: 2020-03-17T15:56:21Z
Registry Expiry Date: 2021-03-17T15:56:21Z
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
```

```
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
```

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: 2020.03.19 09:32:35 -03'00'