Alerta de seguridad informática	8FFR-00152-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	16 de diciembre de 2019
Última revisión	16 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 tres portales fraudulentos asociados a una IP 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 Compromisos

URL´s

URL Sitio Clonado:
https[://]www[.]login-bcoestado[.]cl/banco-estado/comun2019/
https[://]www[.]activacion-banc0estado[.]info/imagenes/comun2008/banca-en-linea-personas[.]php?html
bancoestado[.]sytes[.]net

Domain login-bcoestado.cl

login-bcoestado / cl / Subdomains

record type	TTL	value		
A	14400	162.241.60.178		
NS	86400	ns17.hostgator.cl	Zones on DNS server	162.241.60.176
NS	86400	ns16.hostgator.cl	Zones on DNS server	162.241.60.175
MX	14400	0 mail.login-bcoestado.cl		
TXT	14400	v=spf1 a mx include:websitewelcome.com ~all		
SOA	86400	Mname: ns16.hostgator.cl Rname: root.shared16.hostgator.cl Serial number: 2019121304 Refresh: 86400 Retry: 7200 Expire: 3600000 Minimum TTL: 86400		

Domain activacion-banc0estado.info

activacion-banc0estado / info / Subdomains

record type	TTL	value		
A	7207	139.59.90.115		
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, 45.32.237.128, 168.235.75.52
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: 1576500025 Refresh: 7200 Retry: 1800 Expire: 1209600 Minimum TTL: 600		

Domain sytes.net

sytes / 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	600	10 mail2.no-ip.com		69.65.5.119
TXT	360	v=spf1 include:no-ip.com -all		
SOA	60	Mname	nf1.no-ip.com	
		Rname	hostmaster.no-ip.com	
		Serial number	2086032221	
		Refresh	600	
		Retry	300	
		Expire	604800	
		Minimum TTL	600	

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

Certificados

Basic Information

Subject DN OU=Domain Control Validated, OU=PositiveSSL, CN=login-bcoestado.cl

Issuer DN C=GB, ST=Greater Manchester, L=Salford, O=Sectigo Limited, CN=Sectigo RSA Domain Validation Secure Server CA

Serial 150709637643907521893945343819742390 45

Validity 2019-12-13 00:00:00 **to** 2020-12-12 23:59:59 (365 days, 23:59:59)

Names login-bcoestado.cl
www.login-bcoestado.cl

Basic Information

Subject DN CN=www.activacion-banc0estado.info

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

Serial 348335602941002000942700402862500388073195

Validity 2019-12-14 06:54:32 **to** 2020-03-13 06:54:32 (90 days, 0:00:00)

Names www.activacion-banc0estado.info

Subject DN	CN=bancoestado.sytes.net
Issuer DN	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
Serial	404688826982710598590830057348808009985084
Validity	2019-12-16 14:52:23 **to** 2020-03-15 14:52:23 (90 days, 0:00:00)
Names	bancoestado.sytes.net

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

IP
162.241.60.178
139.59.90.115
104.36.229.103

Domain login-bcoestado.cl is located on IP address << 162.241.60.178 >>

Block start	162.240.0.0
End of block	162.241.255.255
Block size	131072 Domains in block
Block name	UNIFIEDLAYER-NETWORK-16
AS number	46606
Parent block	162.0.0.0 - 162.255.255.255
Organization	UnifiedLayer
City	Provo
Region/State	Utah
Country	US , United States
Reg. date	2013-08-22
Host name	162-241-60-178.unifiedlayer.com
Domains	1 login-bcoestado.cl

Domain activacion-banc0estado.info is located on IP address << 139.59.90.115 >>	
Block start	139.59.0.0
End of block	139.59.255.254
Block size	65535 Domains in block
Block name	DIGITALOCEAN-AP
AS number	14061
Parent block	139.59.0.0 - 139.59.255.255
Organization	DigitalOcean, LLC
Country	SG , Singapore
Host name	no record in reverse zone
Domains	1 activacion-banc0estado.info

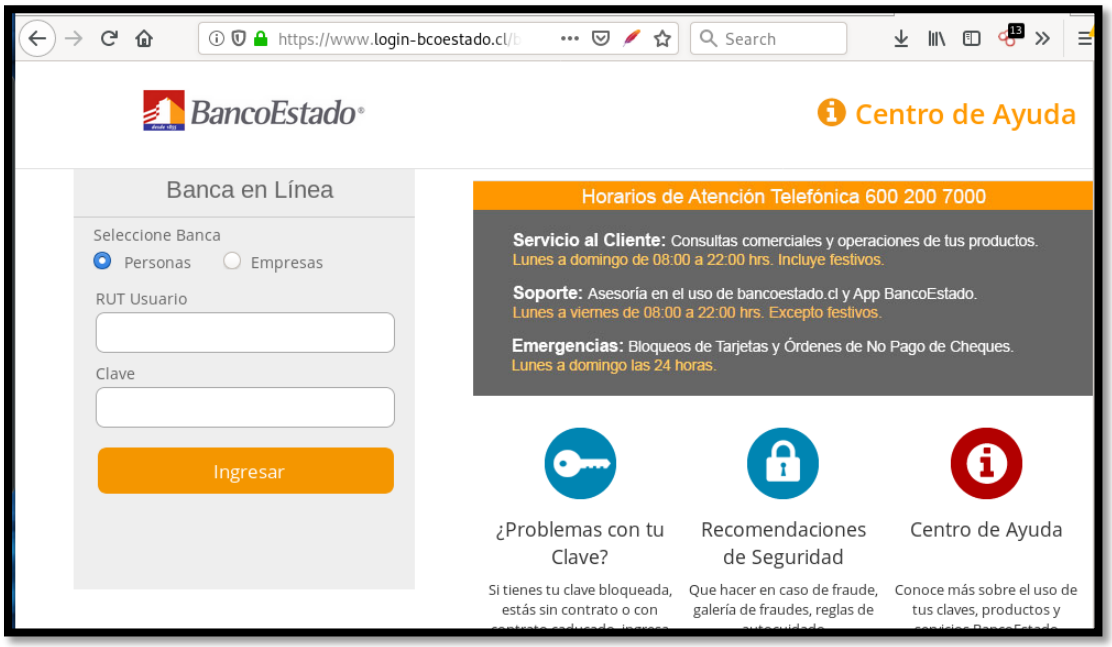
Domain bancoestado.sytes.net is located on IP address << 104.36.229.103 >>	
Block start	104.36.224.0
End of block	104.36.231.255
Block size	2048 Domains in block
Block name	VWEB-6
AS number	395092
Parent block	104.0.0.0 - 104.255.255.255
Organization	Versaweb, LLC
City	Las Vegas
Region/State	Nevada
Country	US , United States
Reg. date	2014-06-05
Host name	no record in reverse zone
Domains	1 bancoestado.sytes.net

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

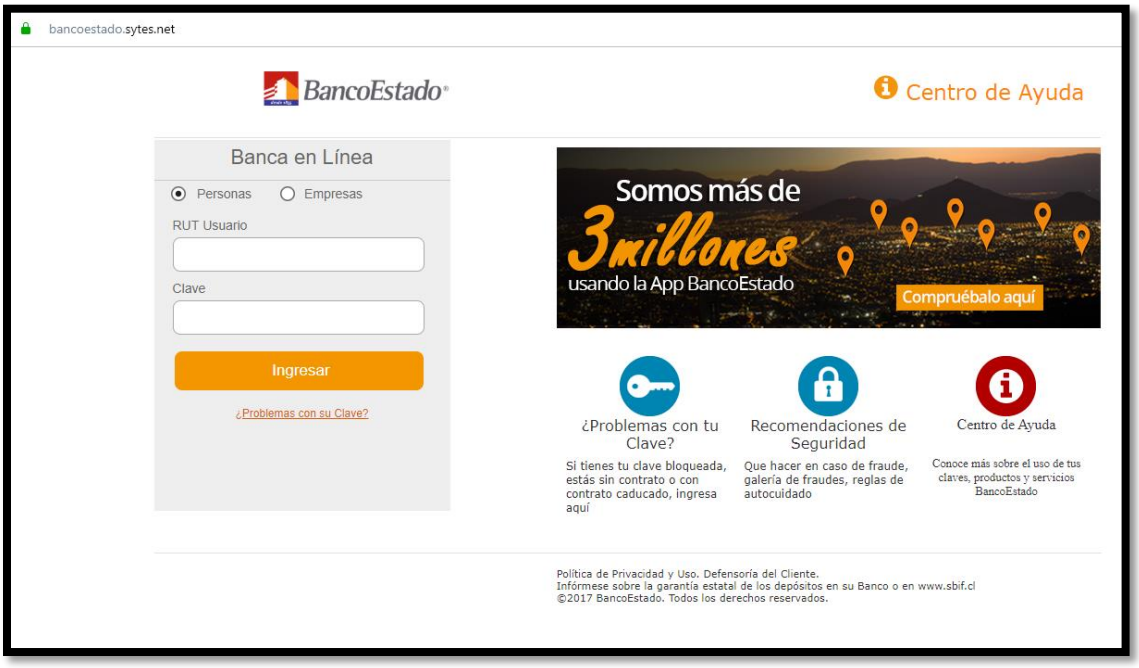
Localización

Provo, Utah, Estados Unidos
Chicago, Illinois, Estados Unidos
Bangalore, Karnataka, India

Imagen del sitio




https://www.activacion-banc0estad
Search
BancoEstado
Centro de Ayuda
Banca en Línea
RUT Usuario
Clave
Ingresar
¿Problemas con su Clave?
Acceso Empresas
Ya somos más de
3.000.000
usando la App BancoEstado
¡Únete tú también
y simplifica tu vida!
¿Problemas con tu Clave?
Si tienes tu clave bloqueada, estás sin contrato o con
Revisa aquí el fraude del momento
¿Qué hacer en caso de fraude?, tipos de fraudes y
Centro de Ayuda
Conoce más sobre el uso de tus claves, productos y


bancoestado.sytes.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
©2017 BancoEstado. Todos los derechos reservados.

Whois

```
Domain name: login-bcoestado.cl
Registrant name: jose avila
Registrant organisation: N/A
Registrar name: PDR Ltd. d/b/a PublicDomainRegistry.com
Registrar URL: https://www.publicdomainregistry.com
Creation date: 2019-12-13 15:23:07 CLST
Expiration date: 2020-12-13 15:23:07 CLST
Name server: ns16.hostgator.cl
Name server: ns17.hostgator.cl
```

```
soc@ITQ-ivps3:~$ whois activacion-banc0estado.info
Domain Name: ACTIVACION-BANC0ESTADO.INFO
Registry Domain ID: D503300001182588466-LRMS
Registrar WHOIS Server: whois.namesilo.com
Registrar URL: http://www.namesilo.com
Updated Date: 2019-12-14T07:15:13Z
Creation Date: 2019-12-14T07:04:51Z
Registry Expiry Date: 2020-12-14T07:04:51Z
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: PREMIUM-NS1.DNSOWL.COM
Name Server: PREMIUM-NS2.DNSOWL.COM
Name Server: PREMIUM-NS3.DNSOWL.COM
DNSSEC: unsigned
```

```
Domain Name: sytes.net
Registry Domain ID: 5534045_DOMAIN_NET-VRSN
Registrar WHOIS Server: whois.srsplus.com
Registrar URL: http://srsplus.com
Updated Date: 2017-01-31T17:05:30Z
Creation Date: 1999-04-22T04:00:00Z
Registrar Registration Expiration Date: 2021-04-22T04:00:00Z
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: nf3.no-ip.com
Name Server: nf2.no-ip.com
Name Server: nf4.no-ip.com
Name Server: nf1.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: 2019.12.16 22:56:50 -03'00'