Alerta de seguridad informática	8FFR20-00201-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	01 de Febrero de 2020
Última revisión	01 de Febrero 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 dos 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

www1[.]bankestado[.]cl[.]tact0[.]info

www1[.]bankestado[.]cl[.]tact0[.]info/imagenes/comun2008/banca-en-linea-personas[.]php?html

redvipervdc[.]com/cream/imagenes/comun2008/banca-en-linea-personas[.]html

Domain tact0.info

tact0 / info / Subdomains

record type	TTL	value		
A	7207	68.183.81.16		
NS	172800	ns1.dnsowl.com	Zones on DNS server	104.207.141.138, 198.251.84.16, 185.34.216.159
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, 209.141.39.150, 45.63.5.234

SOA	172800	Mname	ns1.dnsowl.com
		Rname	hostmaster.dnsowl.com
		Serial number	1580480497
		Refresh	7200
		Retry	1800
		Expire	1209600
		Minimum TTL	600

Domain redvipervdc.com

redvipervdc / com / Subdomains

record type	TTL	value		
A	10800	107.180.29.18		
NS	3600	ns06.domaincontrol.com	Zones on DNS server	173.201.70.3
NS	3600	ns05.domaincontrol.com	Zones on DNS server	97.74.102.3

SOA	3600	Mname	ns05.domaincontrol.com
		Rname	dns.jomax.net
		Serial number	2020010800
		Refresh	28800
		Retry	7200
		Expire	604800
		Minimum TTL	600

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

Certificados

Subject DN	CN=www1.bankestado.cl.tact0.info
Issuer DN	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
Serial	286279660212852116680961904343661058181872
Validity	2020-01-30 16:41:16 **to** 2020-04-29 16:41:16 (90 days, 0:00:00)
Names	www1.bankestado.cl.tact0.info

Subject DN	CN=redvipervdc.com
Issuer DN	C=GB, ST=Greater Manchester, L=Salford, O=Sectigo Limited, CN=Sectigo RSA Domain Validation Secure Server CA
Serial	98327868621594630767584409706711417715
Validity	2020-01-09 00:00:00 **to** 2021-01-08 23:59:59 (365 days, 23:59:59)
Names	redvipervdc.com www.redvipervdc.com

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

IP

68[.]183[.]81[.]16

107[.]180[.]29[.]18

Domain www1.bankestado.cl.tact0.info is located on IP address << 68.183.81.16 >>

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
City	Chatsworth
Region/State	California
Country	US , United States
Reg. date	2005-04-14
Host name	no record in reverse zone
Domains	1 www1.bankestado.cl.tact0.info

Domain redvipervdc.com is located on IP address << 107.180.29.18 >>

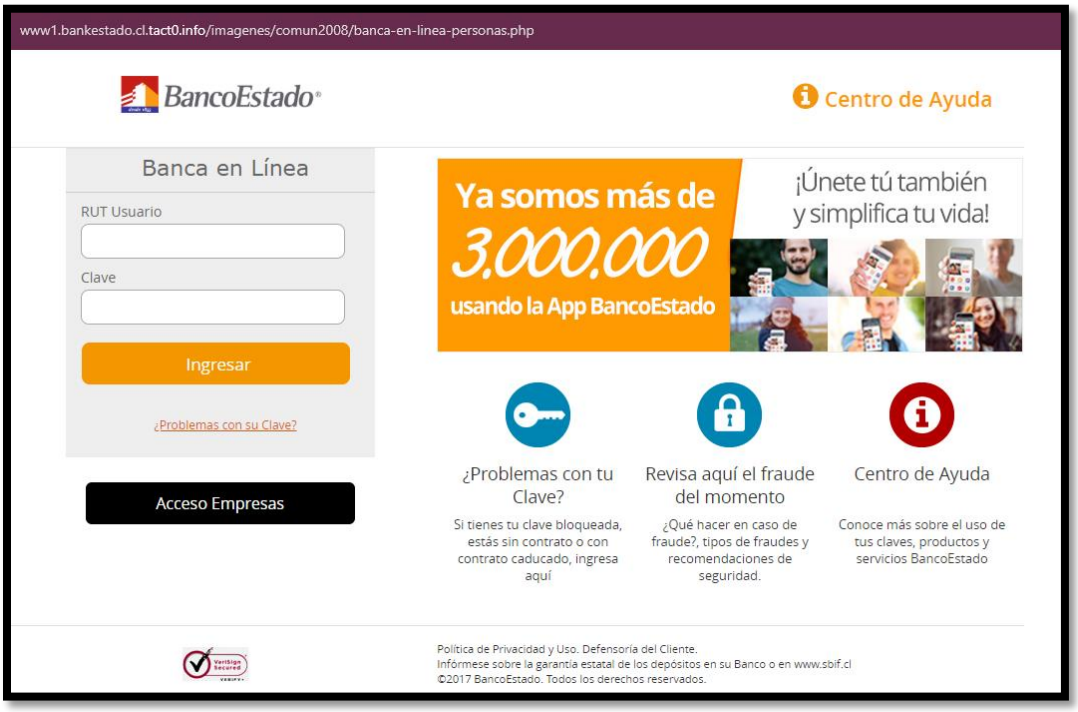
Block start	107.180.0.0
End of block	107.180.127.255
Block size	32768 Domains in block
Block name	GO-DADDY-COM-LLC
AS number	26496
Parent block	107.0.0.0 - 107.255.255.255
Organization	GoDaddy.com, LLC
City	Scottsdale
Region/State	Arizona
Country	US , United States
Reg. date	2014-02-11
Host name	ip-107-180-29-18.ip.secureserver.net
Web server	Apache/2.4.23

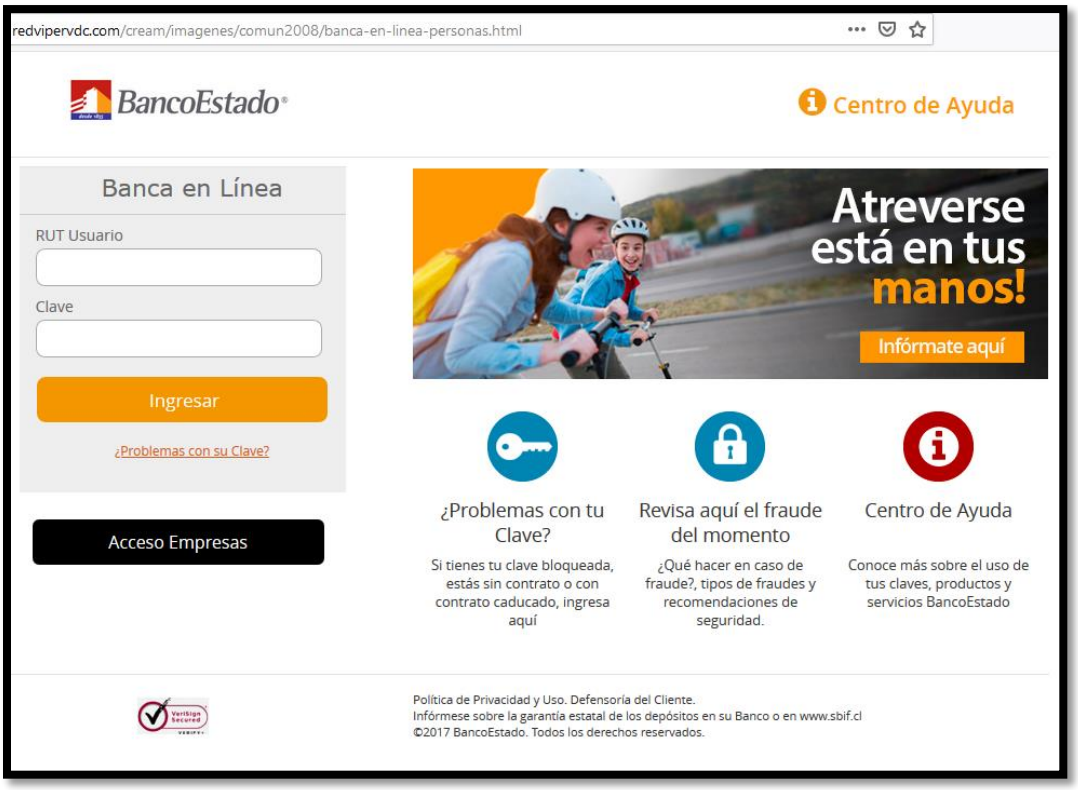
Ilustración 3 Ip de Origen donde se aloja Sitio Falso del Banco Estado.

Localización

Scottdale, Arizona, Estados Unidos
Bangalore, Karnataka, India

Imagen del sitio





Whois

```
Domain Name: TACTO.INFO
Registry Domain ID: D503300001182983431-LRMS
Registrar WHOIS Server: whois.namesilo.com
Registrar URL: http://www.namesilo.com
Updated Date: 2020-01-30T17:30:11Z
Creation Date: 2020-01-30T17:22:52Z
Registry Expiry Date: 2021-01-30T17:22:52Z
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: redvipervdc.com
Registry Domain ID: 2468612342_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: http://www.godaddy.com
Updated Date: 2019-12-18T07:09:16Z
Creation Date: 2019-12-18T07:09:16Z
Registrar Registration Expiration Date: 2021-12-18T07:09:16Z
Registrar: GoDaddy.com, LLC
Registrar IANA ID: 146
Registrar Abuse Contact Email: abuse@godaddy.com
Registrar Abuse Contact Phone: +1.4806242505
Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited http://www.icann.org/epp#clientUpdateProhibited
Domain Status: clientRenewProhibited http://www.icann.org/epp#clientRenewProhibited
Domain Status: clientDeleteProhibited http://www.icann.org/epp#clientDeleteProhibited
Registrant Organization:
Registrant State/Province: Illinois
Registrant Country: US
Registrant Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=redvi
pervdc.com
Admin Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=redvipervd
c.com
Tech Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=redvipervdc
.com
Name Server: NS05.DOMAINCONTROL.COM
Name Server: NS06.DOMAINCONTROL.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: 2020.02.01 12:07:56 -03'00'