Alerta de seguridad informática	8FFR-00134-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	30 de Noviembre de 2019
Última revisión	30 de Noviembre 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 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 Compromisos

URL´s

URL Sitio Clonado:
http[://]visa-homer[.]com/bancoestado/index[.]html[.]html
https[://]www[.]bamcoestado-cl[.]site/imagenes/comun2008/banca-en-linea-personas[.]php?html

Domain bamcoestado-cl.site

bamcoestado-cl / site / Subdomains

record type	TTL	value		
A	7207	206.189.141.0		
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	64.32.22.100, 45.32.237.128, 168.235.75.52
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	1574861110	
		Refresh	7200	
		Retry	1800	
		Expire	1209600	
		Minimum TTL	600	

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

Certificados

Criteria: Identity = 'visa-homer.com'

Certificates

crt.sh ID	Logged At	Not Before	Not After	Issuer Name
2104464324	2019-11-12	2019-11-12	2020-02-10	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
2104464285	2019-11-12	2019-11-12	2020-02-10	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3

www.bamcoestado-cl.site

Certificate | Trust | CT | ZLint | PEM

Basic Information

Subject DN	CN=www.bamcoestado-cl.site
Issuer DN	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
Serial	346082370151507253889846363451815863863355
Validity	2019-11-27 08:01:53 to 2020-02-25 08:01:53 (90 days, 0:00:00)
Names	www.bamcoestado-cl.site

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

IP

162.241.60.177

206.189.141.0

IP address
<< 162.241.60.177 >>

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	162-241-60-177.unifiedlayer.com
Domains	not found

Domain bamcoestado-cl.site is located on IP address
<< 206.189.141.0 >>

Block start	206.189.0.0
End of block	206.189.255.255
Block size	65536 Domains in block
Block name	PILOT-NETBLK-3
AS number	14061
Parent block	206.0.0.0 - 206.255.255.255
Organization	Pilot Network Services, Inc
City	Alameda
Region/State	California
Country	US , United States
Reg. date	1995-11-15
Host name	no record in reverse zone
Domains	1 bamcoestado-cl.site

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

Localización

Provo, Utha, Estados Unidos

Alameda, California, Estados Unidos

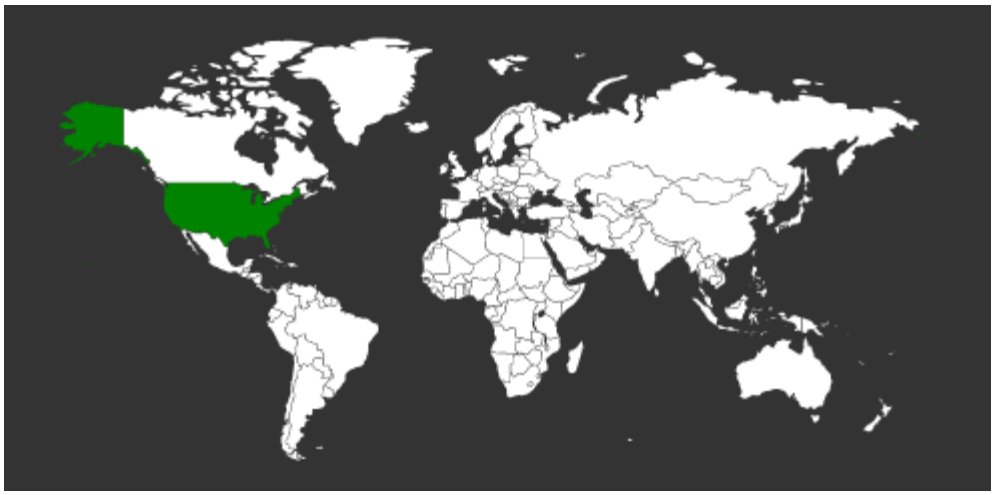
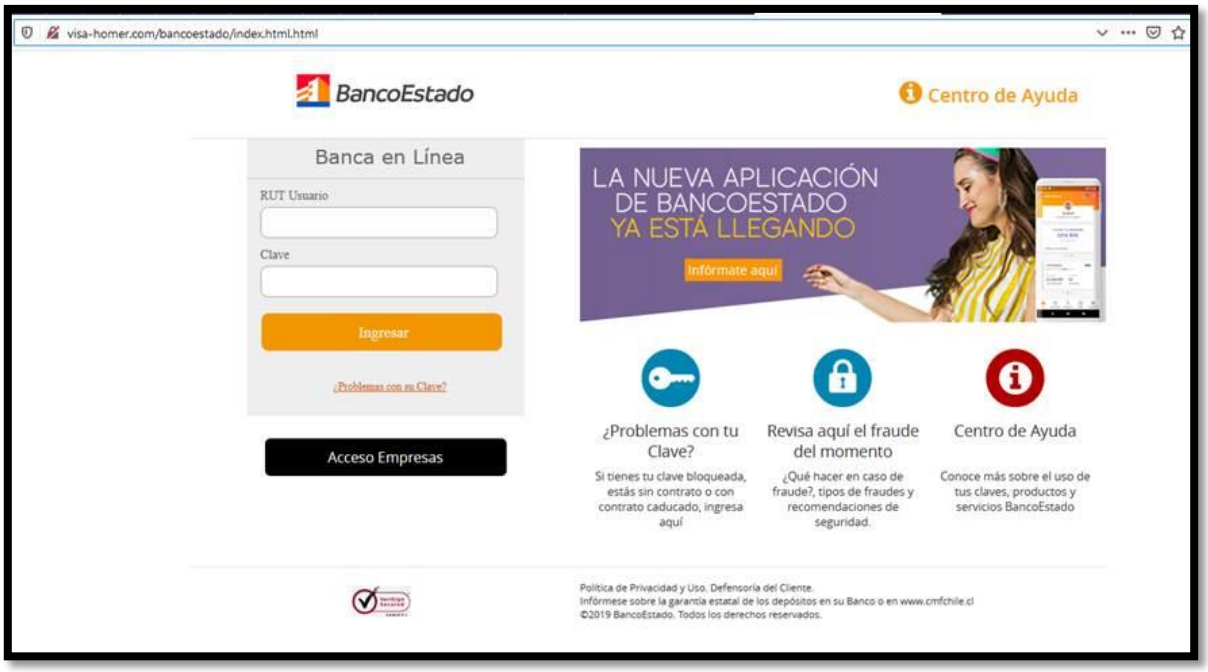
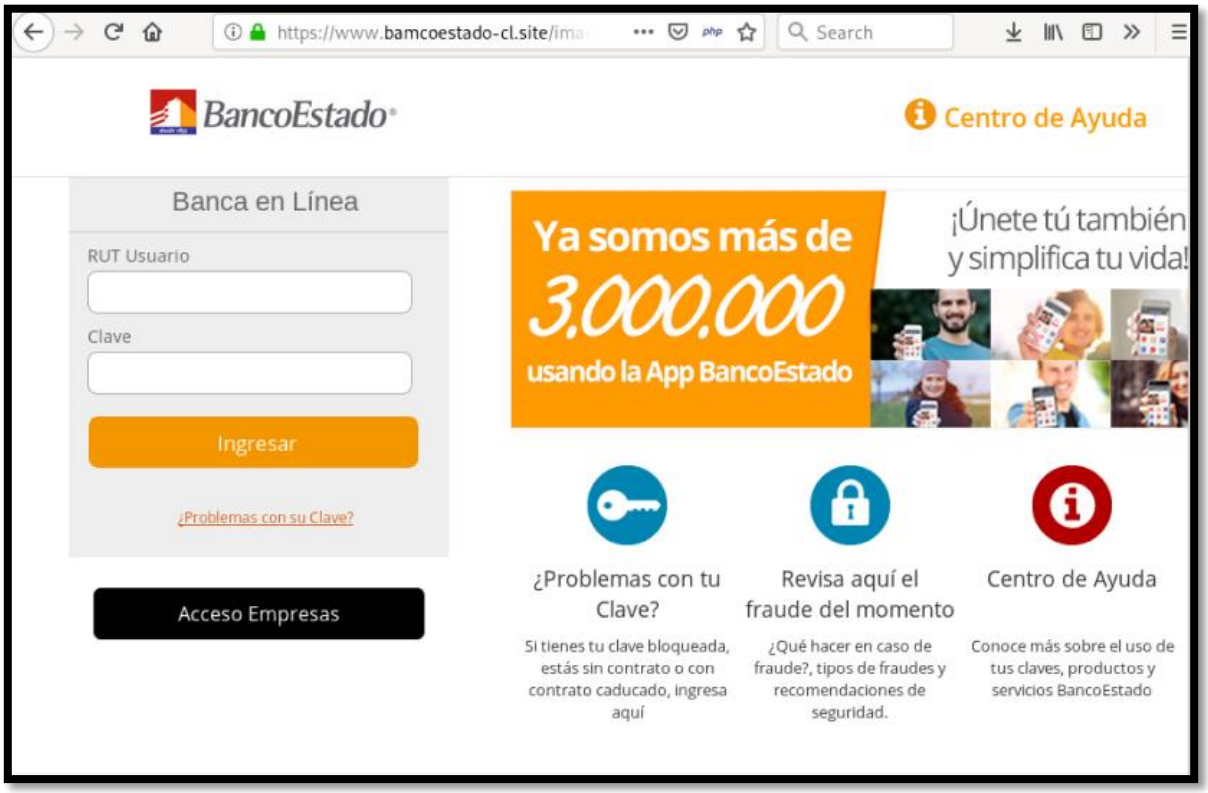


Imagen del sitio





Whois

```
Domain Name: VISA-HOMER.COM
Registry Domain ID: 2454499020_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.publicdomainregistry.com
Registrar URL: www.publicdomainregistry.com
Updated Date: 2019-11-27T13:01:31Z
Creation Date: 2019-11-12T23:52:27Z
Registrar Registration Expiration Date: 2020-11-12T23:52:27Z
Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com
Registrar IANA ID: 303
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Domain Status: clientHold https://icann.org/epp#clientHold
Registry Registrant ID: Not Available From Registry
Registrant Name: jose perez
Registrant Organization:
Registrant Street: el vergel 324, 32423 cerro navia
Registrant City: Cerro Navia
Registrant State/Province: RM
Registrant Postal Code: 8320000
Registrant Country: CL
Registrant Phone: +56.973748237
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: joseperezcnc4@gmail.com
Registry Admin ID: Not Available From Registry
Admin Name: jose perez
Admin Organization:
Admin Street: el vergel 324, 32423 cerro navia
Admin City: Cerro Navia
Admin State/Province: RM
Admin Postal Code: 8320000
Admin Country: CL
Admin Phone: +56.973748237
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: joseperezcnc4@gmail.com
Registry Tech ID: Not Available From Registry
Tech Name: jose perez
Tech Organization:
Tech Street: el vergel 324, 32423 cerro navia
Tech City: Cerro Navia
Tech State/Province: RM
Tech Postal Code: 8320000
Tech Country: CL
Tech Phone: +56.973748237
Tech Phone Ext:
Tech Fax:
Tech Fax Ext:
Tech Email: joseperezcnc4@gmail.com
Name Server: ns1.suspended-domain.com
Name Server: ns2.suspended-domain.com
DNSSEC: Unsigned
Registrar Abuse Contact Email: abuse-contact@publicdomainregistry.com
Registrar Abuse Contact Phone: +1.2013775952
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2019-11-27T13:42:48Z <<<

For more information on Whois status codes, please visit https://icann.org/epp
```

```
Domain Name: bamcoestado-cl.site
Registry Domain ID: D148127981-CNIC
Registrar WHOIS Server: whois.namesilo.com
Registrar URL: https://www.namesilo.com/
Updated Date: 2019-11-27T07:00:00Z
Creation Date: 2019-11-27T07:00:00Z
Registrar Registration Expiration Date: 2020-11-27T07:00:00Z
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-1d887b0b3490e9b600eef75952b2f0e6@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-1d887b0b3490e9b600eef75952b2f0e6@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-1d887b0b3490e9b600eef75952b2f0e6@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/
>>> Last update of WHOIS database: 2019-11-27T07:00:00Z <<<

For more information on Whois status codes, please visit https://icann.org/epp

NOTICE AND TERMS OF USE: You are not authorized to access or query our WHOIS
```

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: 2019.11.30 11:01:08 -03'00'