Alerta de seguridad informática	8FFR-00140-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	05 de Diciembre de 2019
Última revisión	05 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 cinco 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:
www[.]importante-chile[.]pedidomaria[.]com/profesional
www[.]importante-chile[.]pedidomaria[.]com/profesional/imagenes/comun2008/banca-en-linea-personas[.]html
banstados[.]com
banstados[.]com/imagenes/_personas/home/default[.]html
banstados[.]com/imagenes/comun2008/banca-en-linea-personas[.]html

Domain pedidomaria.com

pedidomaria / com / Subdomains

record type	TTL	value		
A	14400	201.159.169.120		
NS	86400	ns30.tecnoinver.cl	Zones on DNS server	201.159.169.120
NS	86400	ns31.tecnoinver.cl	Zones on DNS server	201.159.169.120
MX	14400	0 pedidomaria.com		
TXT	14400	v=spf1 +a +mx +ip4:45.236.164.50 ~all		

SOA	86400	Mname	ns30.tecnoinver.cl
		Rname	reportes.tecnoinver.cl
		Serial number	2019120310
		Refresh	3600
		Retry	1800
		Expire	1209600
		Minimum TTL	86400

Domain banstados.com

banstados / com / Subdomains

record type	TTL	value		
A	10800	107.180.46.151		
NS	3600	ns70.domaincontrol.com	Zones on DNS server	173.201.72.45
NS	3600	ns69.domaincontrol.com	Zones on DNS server	97.74.104.45

SOA	3600	Mname	ns69.domaincontrol.com
		Rname	dns.jomax.net
		Serial number	2019120401
		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=importante-chile.pedidomaria.com
Issuer DN	C=US, ST=TX, L=Houston, O=cPanel, Inc., CN=cPanel, Inc. Certification Authority
Serial	252021117880558656414493765171646984655
Validity	2019-12-03 00:00:00 **to** 2020-03-02 23:59:59 (90 days, 23:59:59)
Names	importante-chile.pedidomaria.com www.importante-chile.pedidomaria.com

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

IP

201.159.169.120

107.180.46.151

Domain pedidomaria.com is located on IP address << 201.159.169.120 >>

Block start	201.159.168.0
End of block	201.159.175.255
Block size	2048 Domains in block
Block name	
AS number	262256
Parent block	201.0.0.0 - 201.255.255.255
Organization	Servicios Informáticos Hostname Ltda
City	Santiago
Region/State	Region Metropolitana de Santiago
Country	CL , Chile
Reg. date	2014-06-06
Host name	guaviare.tecnoinver.cl

Domain banstados.com is located on IP address << 107.180.46.151 >>

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-107-180-46-151.ip.secureserver.net
Web server	Apache/2.4.23
Powered by	PHP/5.6.28

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

Localización

Santiago, Region Metropolitana de Santiago, Chile

Scottsdale, Arizona, Estados Unidos

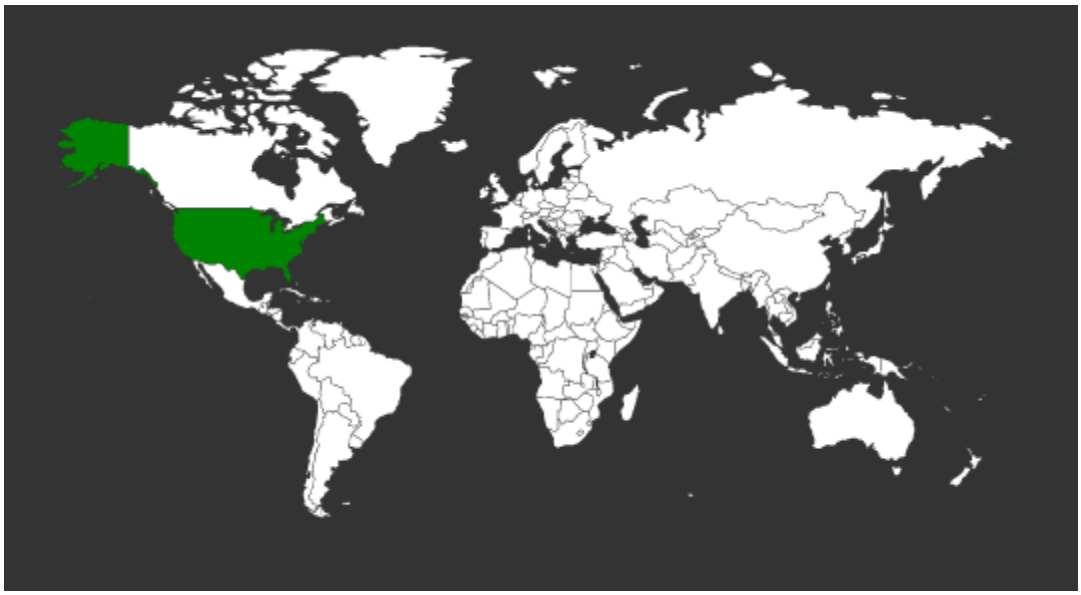
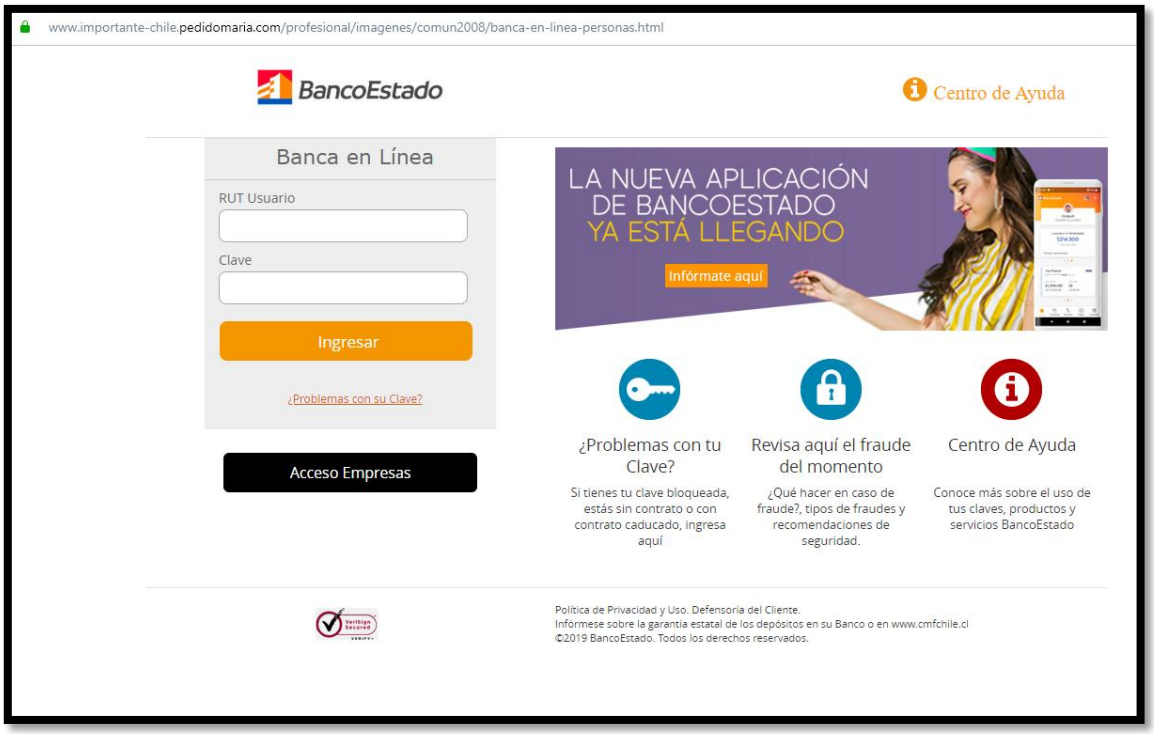
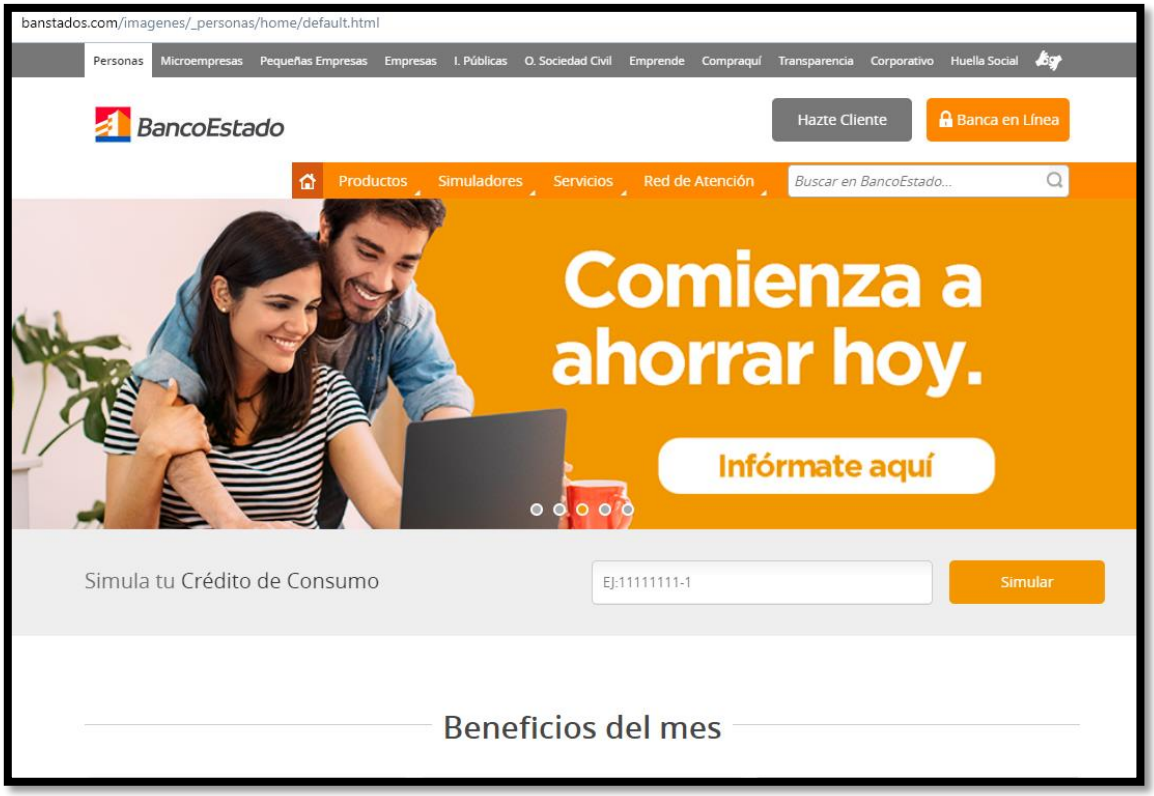


Imagen del sitio





Whois

```
Domain Name: pedidomaria.com
Registry Domain ID: 2458283642_DOMAIN_COM-VRSN
Registrar WHOIS Server: WHOIS.ENOM.COM
Registrar URL: WWW.ENOM.COM
Updated Date: 2019-11-22T15:27:03.00Z
Creation Date: 2019-11-22T15:26:03.00Z
Registrar Registration Expiration Date: 2020-11-22T15:26:03.00Z
Registrar: ENOM, INC.
Registrar IANA ID: 48
Domain Status: clientTransferProhibited https://www.icann.org/epp#clientTransferProhibited
Registrant Name: REDACTED FOR PRIVACY
Registrant Organization: REDACTED FOR PRIVACY
Registrant Street: REDACTED FOR PRIVACY
Registrant Street:
Registrant City: REDACTED FOR PRIVACY
Registrant State/Province: RM
Registrant Postal Code: REDACTED FOR PRIVACY
Registrant Country: CL
Registrant Phone: REDACTED FOR PRIVACY
Registrant Phone Ext:
Registrant Fax: REDACTED FOR PRIVACY
Registrant Email: https://tieredaccess.com/contact/fd2772ff-319d-4ad8-8f52-96454dc64723
Admin Name: REDACTED FOR PRIVACY
Admin Organization: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
Admin Street:
Admin City: REDACTED FOR PRIVACY
Admin State/Province: REDACTED FOR PRIVACY
Admin Postal Code: REDACTED FOR PRIVACY
Admin Country: REDACTED FOR PRIVACY
Admin Phone: REDACTED FOR PRIVACY
Admin Phone Ext:
Admin Fax: REDACTED FOR PRIVACY
Admin Email: REDACTED FOR PRIVACY
Tech Name: REDACTED FOR PRIVACY
Tech Organization: REDACTED FOR PRIVACY
Tech Street: REDACTED FOR PRIVACY
Tech Street:
Tech City: REDACTED FOR PRIVACY
Tech State/Province: REDACTED FOR PRIVACY
Tech Postal Code: REDACTED FOR PRIVACY
Tech Country: REDACTED FOR PRIVACY
Tech Phone: REDACTED FOR PRIVACY
Tech Phone Ext:
Tech Fax: REDACTED FOR PRIVACY
Tech Email: REDACTED FOR PRIVACY
Name Server: NS30.TECNOINVER.CL
Name Server: NS31.TECNOINVER.CL
DNSSEC: unsigned
Registrar Abuse Contact Email: ABUSE@ENOM.COM
Registrar Abuse Contact Phone: +1.4259744689
URL of the ICANN WHOIS Data Problem Reporting System: HTTP://WDPRS.INTERNIC.NET/
>>> Last update of WHOIS database: 2019-12-04T13:36:11.00Z <<<

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

```
Domain Name: banstados.com
Registry Domain ID: 2463189420_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: http://www.godaddy.com
Updated Date: 2019-12-04T09:20:43Z
Creation Date: 2019-12-04T09:20:43Z
Registrar Registration Expiration Date: 2020-12-04T09:20:43Z
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#clientTransferP
rohibited
Domain Status: clientUpdateProhibited http://www.icann.org/epp#clientUpdateProhi
bited
Domain Status: clientRenewProhibited http://www.icann.org/epp#clientRenewProhibi
ted
Domain Status: clientDeleteProhibited http://www.icann.org/epp#clientDeleteProhi
bited
Registrant Organization:
Registrant State/Province: Florida
Registrant Country: US
Registrant Email: Select Contact Domain Holder link at https://www.godaddy.com/w
hois/results.aspx?domain=banstados.com
Admin Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/
results.aspx?domain=banstados.com
Tech Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/r
esults.aspx?domain=banstados.com
Name Server: NS69.DOMAINCONTROL.COM
Name Server: NS70.DOMAINCONTROL.COM
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2019-12-04T14:00:00Z <<<

For more information on Whois status codes, please visit https://www.icann.org/r
esources/pages/epp-status-codes-2014-06-16-en

Notes:

IMPORTANT: Port43 will provide the ICANN-required minimum data set per
ICANN Temporary Specification, adopted 17 May 2018.
Visit https://whois.godaddy.com to look up contact data for domains
not covered by GDPR policy.

The data contained in GoDaddy.com, LLC's WhoIs database,
while believed by the company to be reliable, is provided "as is"
with no guarantee or warranties regarding its accuracy.  This
information is provided for the sole purpose of assisting you
in obtaining information about domain name registration records.
Any use of this data for any other purpose is expressly forbidden without the pr
ior written
permission of GoDaddy.com, LLC.  By submitting an inquiry,
you agree to these terms of usage and limitations of warranty.  In particular,
you agree not to use this data to allow, enable, or otherwise make possible,
dissemination or collection of this data, in part or in its entirety, for any
purpose, such as the transmission of unsolicited advertising and
and solicitations of any kind, including spam.  You further agree
not to use this data to enable high volume, automated or robotic electronic
processes designed to collect or compile this data for any purpose,
including mining this data for your own personal or commercial purposes.
```

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: 2019.12.05 11:07:00 -03'00'