Alerta de seguridad informática	8FFR20-00271-01
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 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

bencoestadopersonal[.]enlinease[.]com
bancoestadomovil[.]com
bancoestadoweb[.]com

Domain enlinease.com

enlinease / com / Subdomains

record type	TTL	value		
A	14400	66.235.200.145		
NS	86400	ns2.bluehost.com	Zones on DNS server	162.159.25.175
NS	86400	ns1.bluehost.com	Zones on DNS server	162.159.24.80
MX	14400	0 mail.enlinease.com		
TXT	14400	v=spf1 a mx include:websitewelcome.com ~all		

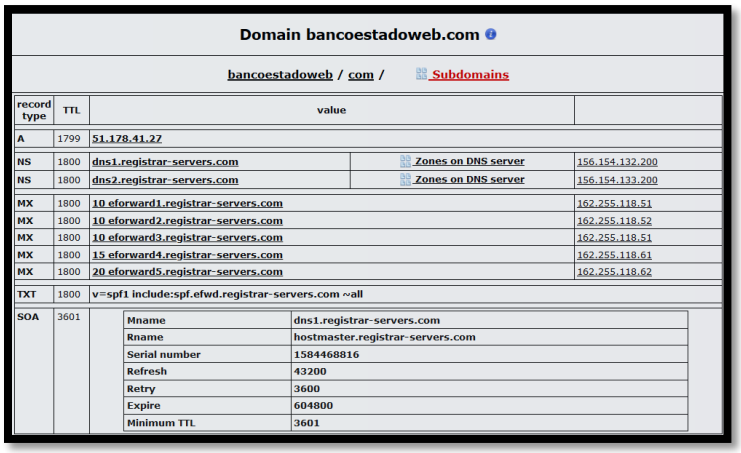
SOA	86400	Mname	ns1.bluehost.com
		Rname	root.box5790.bluehost.com
		Serial number	2020031700
		Refresh	86400
		Retry	7200
		Expire	3600000
		Minimum TTL	300

Domain bancoestadomovil.com

bancoestadomovil / com / Subdomains

record type	TTL	value		
A	1799	51.38.189.136		
NS	1800	dns1.registrar-servers.com	Zones on DNS server	156.154.132.200
NS	1800	dns2.registrar-servers.com	Zones on DNS server	156.154.133.200
MX	1800	10 eforward1.registrar-servers.com		162.255.118.51
MX	1800	10 eforward2.registrar-servers.com		162.255.118.52
MX	1800	10 eforward3.registrar-servers.com		162.255.118.51
MX	1800	15 eforward4.registrar-servers.com		162.255.118.61
MX	1800	20 eforward5.registrar-servers.com		162.255.118.62
TXT	1800	v=spf1 include:spf.efwd.registrar-servers.com ~all		

SOA	3601	Mname	dns1.registrar-servers.com
		Rname	hostmaster.registrar-servers.com
		Serial number	1584490535
		Refresh	43200
		Retry	3600
		Expire	604800
		Minimum TTL	3601



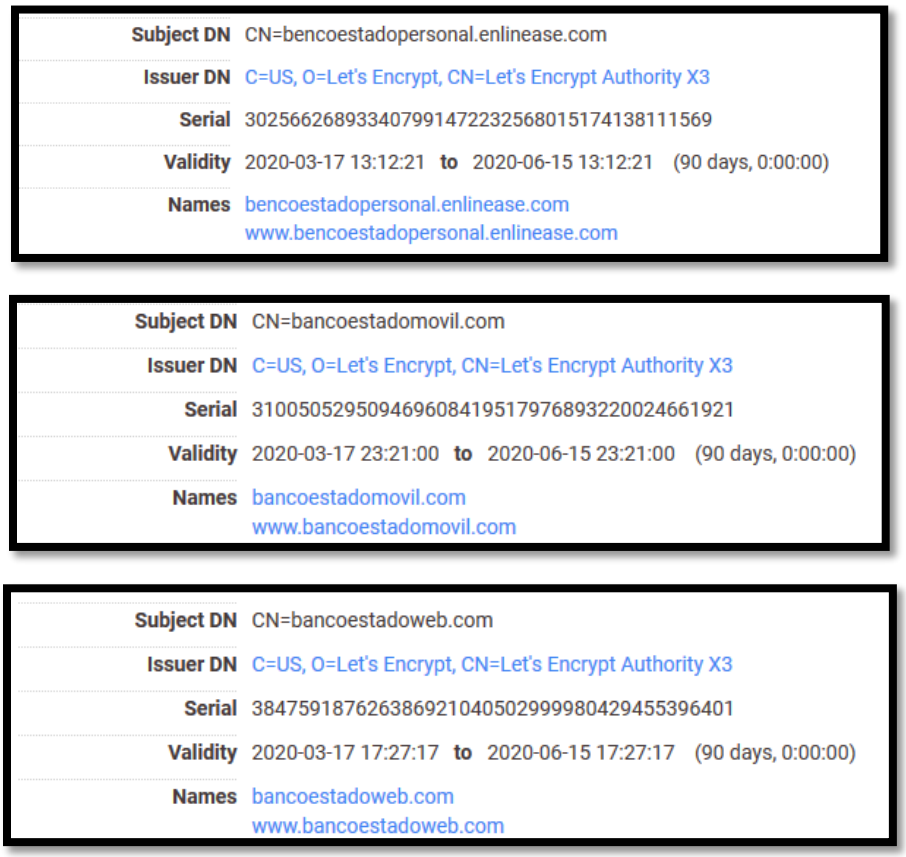
Domain bancoestadoweb.com

bancoestadoweb / com / Subdomains

record type	TTL	value		
A	1799	51.178.41.27		
NS	1800	dns1.registrar-servers.com	Zones on DNS server	156.154.132.200
NS	1800	dns2.registrar-servers.com	Zones on DNS server	156.154.133.200
MX	1800	10 eforward1.registrar-servers.com		162.255.118.51
MX	1800	10 eforward2.registrar-servers.com		162.255.118.52
MX	1800	10 eforward3.registrar-servers.com		162.255.118.51
MX	1800	15 eforward4.registrar-servers.com		162.255.118.61
MX	1800	20 eforward5.registrar-servers.com		162.255.118.62
TXT	1800	v=spf1 include:spf.efwd.registrar-servers.com ~all		
SOA	3601	Mname: dns1.registrar-servers.com Rname: hostmaster.registrar-servers.com Serial number: 1584468816 Refresh: 43200 Retry: 3600 Expire: 604800 Minimum TTL: 3601		

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

Certificados



Subject DN CN=bencoestadopersonal.enlinease.com

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

Serial 302566268933407991472232568015174138111569

Validity 2020-03-17 13:12:21 **to** 2020-06-15 13:12:21 (90 days, 0:00:00)

Names bencoestadopersonal.enlinease.com
www.bencoestadopersonal.enlinease.com

Subject DN CN=bancoestadomovil.com

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

Serial 3100505295094696084195179768932200246619 21

Validity 2020-03-17 23:21:00 **to** 2020-06-15 23:21:00 (90 days, 0:00:00)

Names bancoestadomovil.com
www.bancoestadomovil.com

Subject DN CN=bancoestadoweb.com

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

Serial 384759187626386921040502999980429455396401

Validity 2020-03-17 17:27:17 **to** 2020-06-15 17:27:17 (90 days, 0:00:00)

Names bancoestadoweb.com
www.bancoestadoweb.com

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

IP

162[.]241[.]253[.]120
51[.]38[.]189[.]136
51[.]178[.]41[.]27

Domain bencoestadopersonal.enlinease.com is located on IP address << 162.241.253.120 >>

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

Domain bancoestadomovil.com is located on IP address << 51.38.189.136 >>

Block start	51.38.184.0
End of block	51.38.191.255
Block size	2048 Domains in block
Block name	VPS-GRA
AS number	16276
Parent block	51.38.0.0 - 51.38.255.255
Organization	ORG-OS3-RIPE

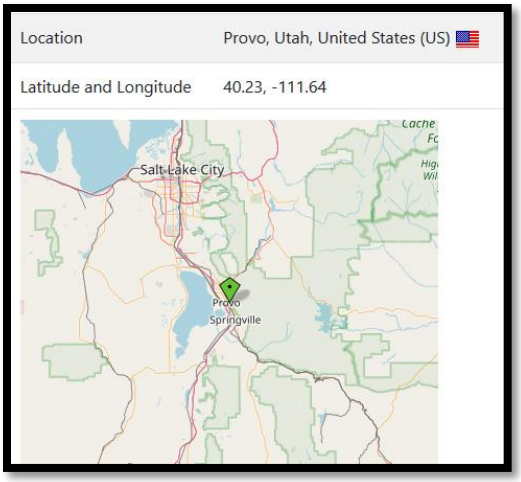
Domain bancoestadoweb.com is located on IP address << 51.178.41.27 >>

Block start	51.178.40.0
End of block	51.178.43.255
Block size	1024 Domains in block
Block name	VPS-GRA8
AS number	16276
Parent block	51.178.0.0 - 51.178.255.255
Organization	ORG-OS3-RIPE

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

Localización

Provo, Utah, Estados Unidos
Roubaix, Hauts-de-France, Francia



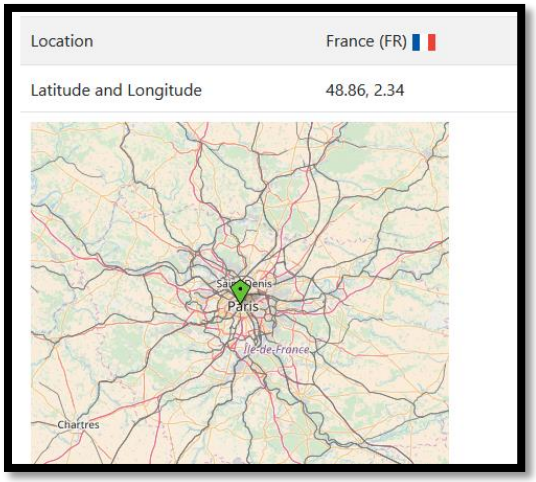
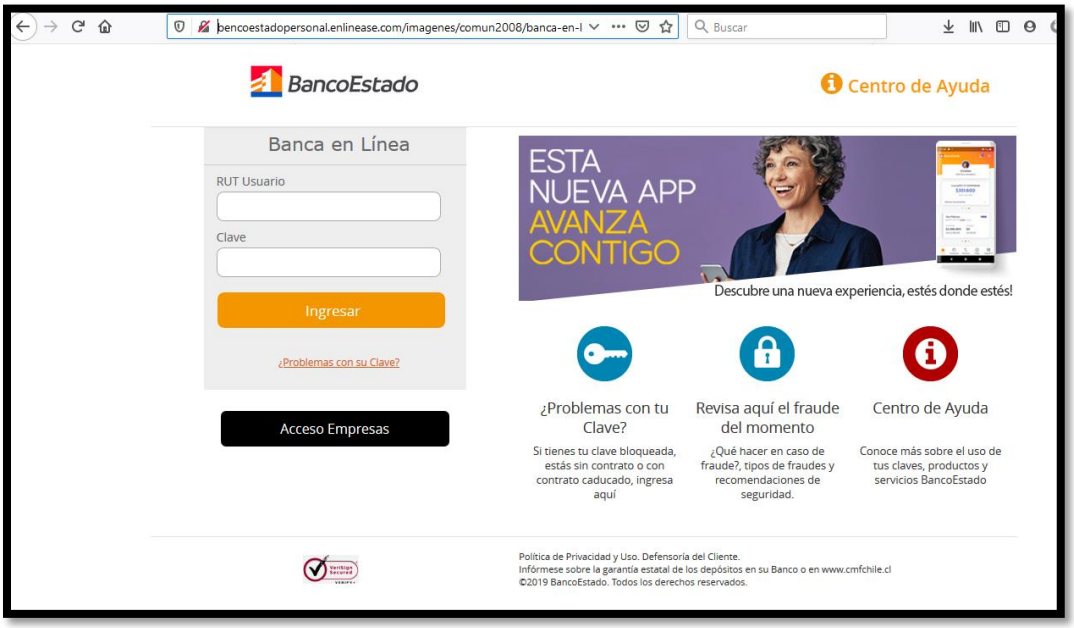
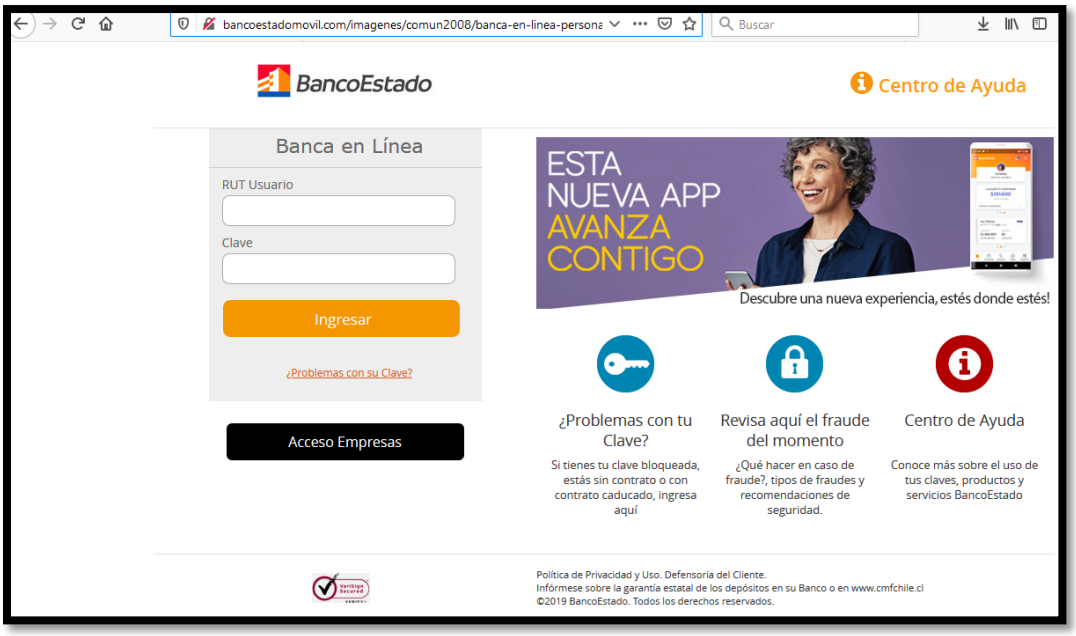
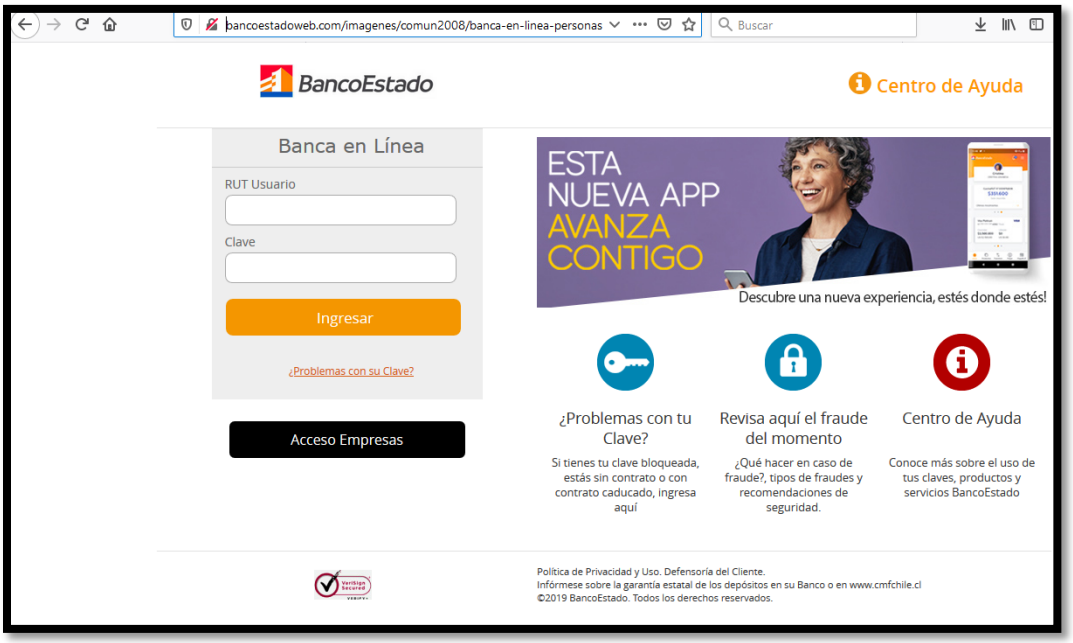


Imagen del sitio




bancoestadomovil.com/imagenes/comun2008/banca-en-linea-persona
Buscar
BancoEstado
Centro de Ayuda
Banca en Línea
RUT Usuario
Clave
Ingresar
¿Problemas con su Clave?
Acceso Empresas
ESTA NUEVA APP AVANZA CONTIGO
Descubre una nueva experiencia, estés donde estés!
¿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.


bancoestadoweb.com/imagenes/comun2008/banca-en-linea-personas
Buscar
BancoEstado
Centro de Ayuda
Banca en Línea
RUT Usuario
Clave
Ingresar
¿Problemas con su Clave?
Acceso Empresas
ESTA NUEVA APP AVANZA CONTIGO
Descubre una nueva experiencia, estés donde estés!
¿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.

Whois

```
Domain Name: ENLINEASE.COM
Registry Domain ID: 2503457753_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.bluehost.com
Registrar URL: http://www.bluehost.com/
Updated Date: 2020-03-14T20:26:14Z
Creation Date: 2020-03-14T20:26:14Z
Registrar Registration Expiration Date: 2021-03-14T20:26:14Z
Registrar: FastDomain Inc.
Registrar IANA ID: 1154
Registrar Abuse Contact Email: support@bluehost.com
Registrar Abuse Contact Phone: +1.8017659400
Reseller: BlueHost.Com
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Registry Registrant ID:
Registrant Name: DOMAIN PRIVACY SERVICE FBO REGISTRANT
Registrant Organization: THE ENDURANCE INTERNATIONAL GROUP, INC.
Registrant Street: 10 CORPORATE DR, STE 300
Registrant City: BURLINGTON
Registrant State/Province: MASSACHUSETTS
Registrant Postal Code: 01803
Registrant Country: US
Registrant Phone: +1.8017659400
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: WHOIS@BLUEHOST.COM
Registry Admin ID:
Admin Name: DOMAIN PRIVACY SERVICE FBO REGISTRANT
Admin Organization: THE ENDURANCE INTERNATIONAL GROUP, INC.
Admin Street: 10 CORPORATE DR, STE 300
Admin City: BURLINGTON
Admin State/Province: MASSACHUSETTS
Admin Postal Code: 01803
Admin Country: US
Admin Phone: +1.8017659400
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: WHOIS@BLUEHOST.COM
Registry Tech ID:
Tech Name: DOMAIN PRIVACY SERVICE FBO REGISTRANT
Tech Organization: THE ENDURANCE INTERNATIONAL GROUP, INC.
Tech Street: 10 CORPORATE DR, STE 300
Tech City: BURLINGTON
Tech State/Province: MASSACHUSETTS
Tech Postal Code: 01803
Tech Country: US
Tech Phone: +1.8017659400
Tech Phone Ext:
Tech Fax:
Tech Fax Ext:
Tech Email: WHOIS@BLUEHOST.COM
Name Server: NS1.BLUEHOST.COM
Name Server: NS2.BLUEHOST.COM
DNSSEC: unsigned
```

```
Domain name: bancoestadomovil.com
Registry Domain ID: 2504283046_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.namecheap.com
Registrar URL: http://www.namecheap.com
Updated Date: 0001-01-01T00:00:00.00Z
Creation Date: 2020-03-17T15:21:36.00Z
Registrar Registration Expiration Date: 2021-03-17T15:21:36.00Z
Registrar: NAMECHEAP INC
Registrar IANA ID: 1068
Registrar Abuse Contact Email: abuse@namecheap.com
Registrar Abuse Contact Phone: +1.6613102107
Reseller: NAMECHEAP INC
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: addPeriod https://icann.org/epp#addPeriod
Registry Registrant ID:
Registrant Name: WhoisGuard Protected
Registrant Organization: WhoisGuard, Inc.
Registrant Street: P.O. Box 0823-03411
Registrant City: Panama
Registrant State/Province: Panama
Registrant Postal Code:
Registrant Country: PA
Registrant Phone: +507.8365503
Registrant Phone Ext:
Registrant Fax: +51.17057182
Registrant Fax Ext:
Registrant Email: b7fe02b21c284a83b95a7300f22aac33.protect@whoisguard.com
Registry Admin ID:
Admin Name: WhoisGuard Protected
Admin Organization: WhoisGuard, Inc.
Admin Street: P.O. Box 0823-03411
Admin City: Panama
Admin State/Province: Panama
Admin Postal Code:
Admin Country: PA
Admin Phone: +507.8365503
Admin Phone Ext:
Admin Fax: +51.17057182
Admin Fax Ext:
Admin Email: b7fe02b21c284a83b95a7300f22aac33.protect@whoisguard.com
Registry Tech ID:
Tech Name: WhoisGuard Protected
Tech Organization: WhoisGuard, Inc.
Tech Street: P.O. Box 0823-03411
Tech City: Panama
Tech State/Province: Panama
Tech Postal Code:
Tech Country: PA
Tech Phone: +507.8365503
Tech Phone Ext:
Tech Fax: +51.17057182
Tech Fax Ext:
Tech Email: b7fe02b21c284a83b95a7300f22aac33.protect@whoisguard.com
Name Server: dns1.registrar-servers.com
Name Server: dns2.registrar-servers.com
DNSSEC: unsigned
```

```
Domain Name: BANCOESTADOWEB.COM
Registry Domain ID: 2504283051_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.namecheap.com
Registrar URL: http://www.namecheap.com
Updated Date: 2020-03-17T15:21:43Z
Creation Date: 2020-03-17T15:21:40Z
Registry Expiry Date: 2021-03-17T15:21:40Z
Registrar: NameCheap, Inc.
Registrar IANA ID: 1068
Registrar Abuse Contact Email: abuse@namecheap.com
Registrar Abuse Contact Phone: +1.6613102107
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Name Server: DNS1.REGISTRAR-SERVERS.COM
Name Server: DNS2.REGISTRAR-SERVERS.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 09:07:29 -03'00'