Alerta de seguridad informática	8FFR-00150-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de Diciembre de 2019
Última revisión	14 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 dos 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[.]bamcoestado[.]xyz/imagenes/comun2008/banca-en-linea-personas[.]php?html
https[://]web-banestado-avance-cupo-linea-credito-promo[.]000webhostapp[.]com/portal-accesso-personas/linea-credito-aumento-cupo/estado-promo2019-diciembre/www[.]bancoestado[.]cl/

Domain www.bamcoestado.xyz

www / bamcoestado / xyz / Subdomains

record type	TTL	value
A	7207	139.59.94.8

Domain 000webhostapp.com

000webhostapp / com / Subdomains

record type	TTL	value		
A	60	153.92.0.100		
NS	900	dns2.000webhost.com	Zones on DNS server	153.92.2.20
NS	900	dns1.000webhost.com	Zones on DNS server	153.92.2.10
MX	3600	1 ASPMX.L.GOOGLE.com		
TXT	3600	h0xkmxkckcltwjb7v25vhl8c4xngkmst		
TXT	14400	v=spf1 -all		
TXT	3600	google-site-verification=o8fiVtoqn6PtOerlqmBsJ0dDG0-k7szm03Q3-I_nZ10		

SOA	900	Mname	dns1.000webhost.com
		Rname	hostmaster.000webhost.com
		Serial number	1
		Refresh	7200
		Retry	900
		Expire	1209600
		Minimum TTL	86400

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

Certificados

Basic Information

Subject DN	CN=www.bamcoestado.xyz
Issuer DN	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
Serial	303579353734596897911826069920040421520739
Validity	2019-12-12 06:10:09 **to** 2020-03-11 06:10:09 (90 days, 0:00:00)
Names	www.bamcoestado.xyz

Fingerprint

SHA-256	355069601e8610dbedd739f3539a4517cb97410fb1ddc311c46ebda19acf1f80
SHA-1	54bc57d7329a4d644bc043be4aeb1fac2e701b0d
MD5	dbb549a7065544d713e74aaf17baa61e

Public Key

Key Type	2048-bit RSA, e = 65,537 ✔ STRONG
Modulus	be:6d:8c:08:e1:e1:62:db:50:ec:58:83:e9:f9:8f:28:65:02:d2:47:
SPKI SHA-256	fd9285f1519f0c4a89154b11fa12e0e81292cdc20a4905ae9ab08e440838be46

Criteria	Identity = '000webhostapp.com'; Exclude expired certificates

Certificates

crt.sh ID	Logged At	Not Before	Not After	Issuer Name
1573772898	2019-06-13	2019-06-11	2021-07-10	C=US, O=DigiCert Inc, OU=www.digicert.com, CN=RapidSSL RSA CA 2018
1566039480	2019-06-11	2019-06-11	2021-07-10	C=US, O=DigiCert Inc, OU=www.digicert.com, CN=RapidSSL RSA CA 2018

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

IP

139.59.94.8

153.92.0.100

Domain www.bamcoestado.xyz is located on IP address << 139.59.94.8 >>

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 www.bamcoestado.xyz

Domain 000webhostapp.com is located on IP address << 153.92.0.100 >>

Block start	153.92.0.0
End of block	153.92.15.255
Block size	4096 Domains in block
Block name	HOSTINGER-HOSTING
AS number	204915
Parent block	153.0.0.0 - 153.255.255.255
Organization	ORG-ARTA1-RIPE
City	Charlotte
Region/State	North Carolina
Country	US , United States
Reg. date	1991-09-23
Host name	no record in reverse zone
Domain count	>= 3 Servers around
Domains	1 000webhostapp.com 2 ccshop.comyr.com 3 testing112.comuf.com

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

Localización

Bangalore, Karnataka, India
Charlotte, Carolina de Norte, Estados Unidos

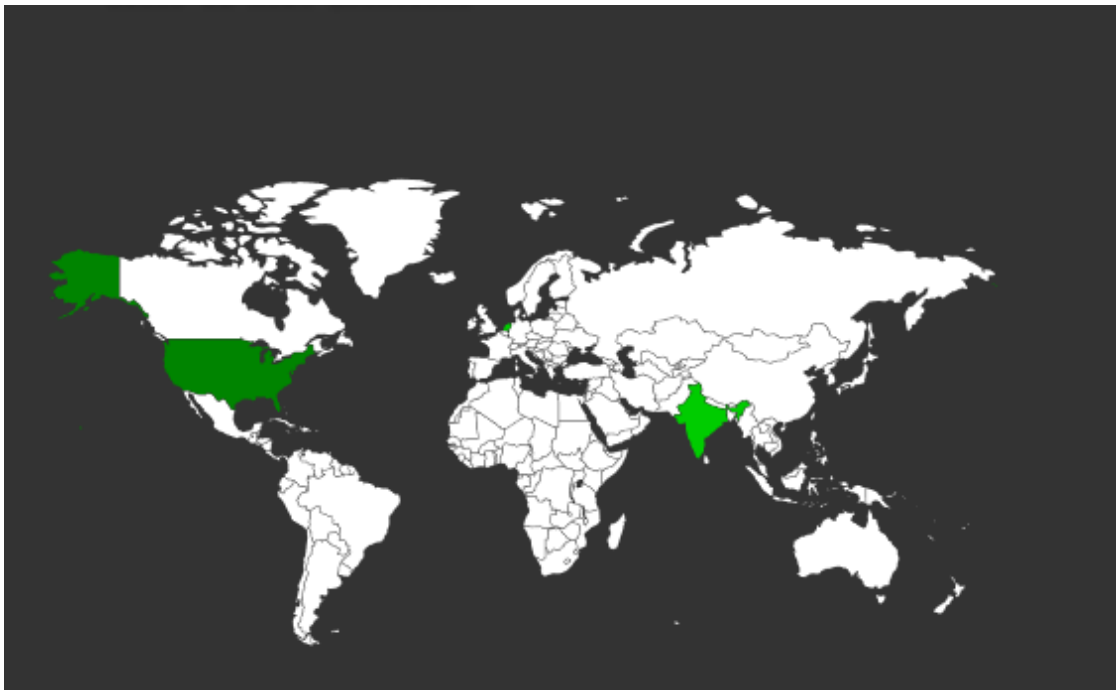
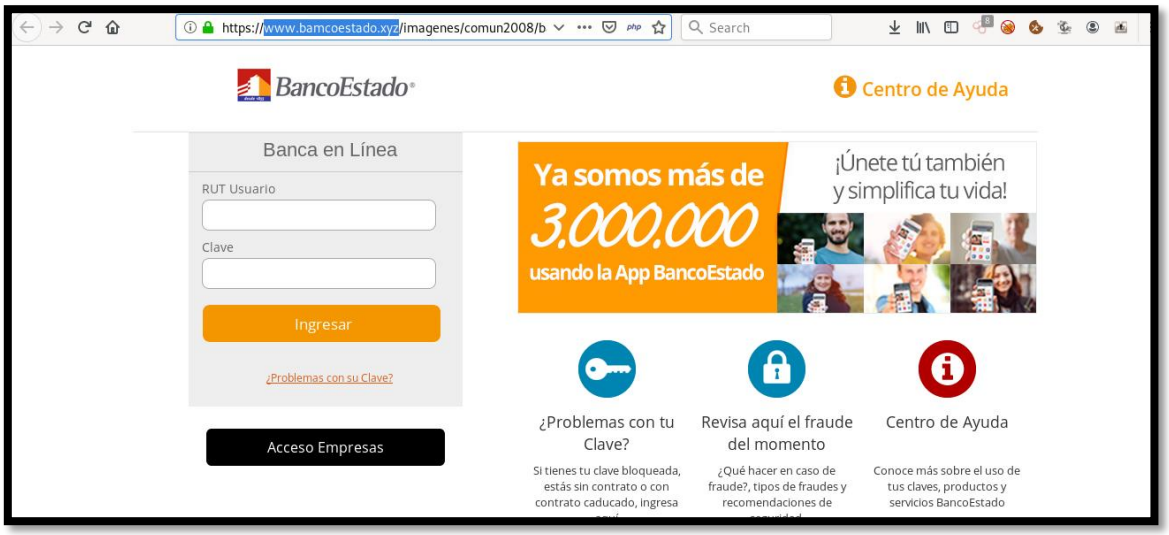


Imagen del sitio



Whois

```
Domain Name: BAMCOESTADO.XYZ
Registry Domain ID: D152063831-CNIC
Registrar WHOIS Server: whois.namesilo.com
Registrar URL: https://www.namesilo.com
Updated Date: 2019-12-12T06:00:34.0Z
Creation Date: 2019-12-12T05:52:58.0Z
Registry Expiry Date: 2020-12-12T23:59:59.0Z
Registrar: NameSilo, LLC
Registrar IANA ID: 1479
Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: addPeriod https://icann.org/epp#addPeriod
Registrant Organization: See PrivacyGuardian.org
Registrant State/Province: AZ
Registrant Country: US
Registrant Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to cont
act the Registrant, Admin, or Tech contact of the queried domain name.
Admin Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact t
he Registrant, Admin, or Tech contact of the queried domain name.
Tech Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact th
e Registrant, Admin, or Tech contact of the queried domain name.
Name Server: NS1.DNSOWL.COM
Name Server: NS2.DNSOWL.COM
Name Server: NS3.DNSOWL.COM
DNSSEC: unsigned
Billing Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact
 the Registrant, Admin, or Tech contact of the queried domain name.
Registrar Abuse Contact Email: abuse@namesilo.com
Registrar Abuse Contact Phone: +1.4805240066
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of WHOIS database: 2019-12-12T15:12:04.0Z <<<

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

>>> IMPORTANT INFORMATION ABOUT THE DEPLOYMENT OF RDAP: please visit
https://www.centralnic.com/support/rdap <<<

The Whois and RDAP services are provided by CentralNic, and contain
information pertaining to Internet domain names registered by our
our customers. By using this service you are agreeing (1) not to use any
information presented here for any purpose other than determining
ownership of domain names, (2) not to store or reproduce this data in
any way, (3) not to use any high-volume, automated, electronic processes
to obtain data from this service. Abuse of this service is monitored and
actions in contravention of these terms will result in being permanently
blacklisted. All data is (c) CentralNic Ltd (https://www.centralnic.com)

Access to the Whois and RDAP services is rate limited. For more
information, visit https://registrar-console.centralnic.com/pub/whois_guidance.
```

```
Domain Name: 000WEBHOSTAPP.COM
Registry Domain ID: 2027404438_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.hostinger.com
Registrar URL: https://www.hostinger.com
Updated Date: 2017-04-05T08:09:44Z
Creation Date: 2016-05-11T13:34:12Z
Registrar Registration Expiration Date: 2022-05-11T13:34:12Z
Registrar: Hostinger, UAB
Registrar IANA ID: 1636
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Registry Registrant ID: Not Available From Registry
Registrant Name: GDPR Masked
Registrant Organization: GDPR Masked
Registrant Street: GDPR Masked GDPR Masked GDPR Masked
Registrant City: GDPR Masked
Registrant State/Province: Larnaka
Registrant Postal Code: GDPR Masked
Registrant Country: CY
Registrant Phone: +GDPR Masked.GDPR Masked
Registrant Phone Ext:
Registrant Fax: +GDPR Masked.GDPR Masked
Registrant Fax Ext:
Registrant Email: gdpr-masking@gdpr-masked.com
Registry Admin ID: Not Available From Registry
Admin Name: GDPR Masked
Admin Organization: GDPR Masked
Admin Street: GDPR Masked GDPR Masked GDPR Masked
Admin City: GDPR Masked
Admin State/Province: Larnaka
Admin Postal Code: GDPR Masked
Admin Country: CY
Admin Phone: +GDPR Masked.GDPR Masked
Admin Phone Ext:
Admin Fax: +GDPR Masked.GDPR Masked
Admin Fax Ext:
Admin Email: gdpr-masking@gdpr-masked.com
Registry Tech ID: Not Available From Registry
Tech Name: GDPR Masked
Tech Organization: GDPR Masked
Tech Street: GDPR Masked GDPR Masked GDPR Masked
Tech City: GDPR Masked
Tech State/Province: Larnaka
Tech Postal Code: GDPR Masked
Tech Country: CY
Tech Phone: +GDPR Masked.GDPR Masked
Tech Phone Ext:
Tech Fax: +GDPR Masked.GDPR Masked
Tech Fax Ext:
Tech Email: gdpr-masking@gdpr-masked.com
Name Server: dns1.000webhost.com
Name Server: dns2.000webhost.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: 2019.12.14 12:06:42 -03'00'