Alerta de seguridad informática	8FFR-00158-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	19 de diciembre de 2019
Última revisión	19 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

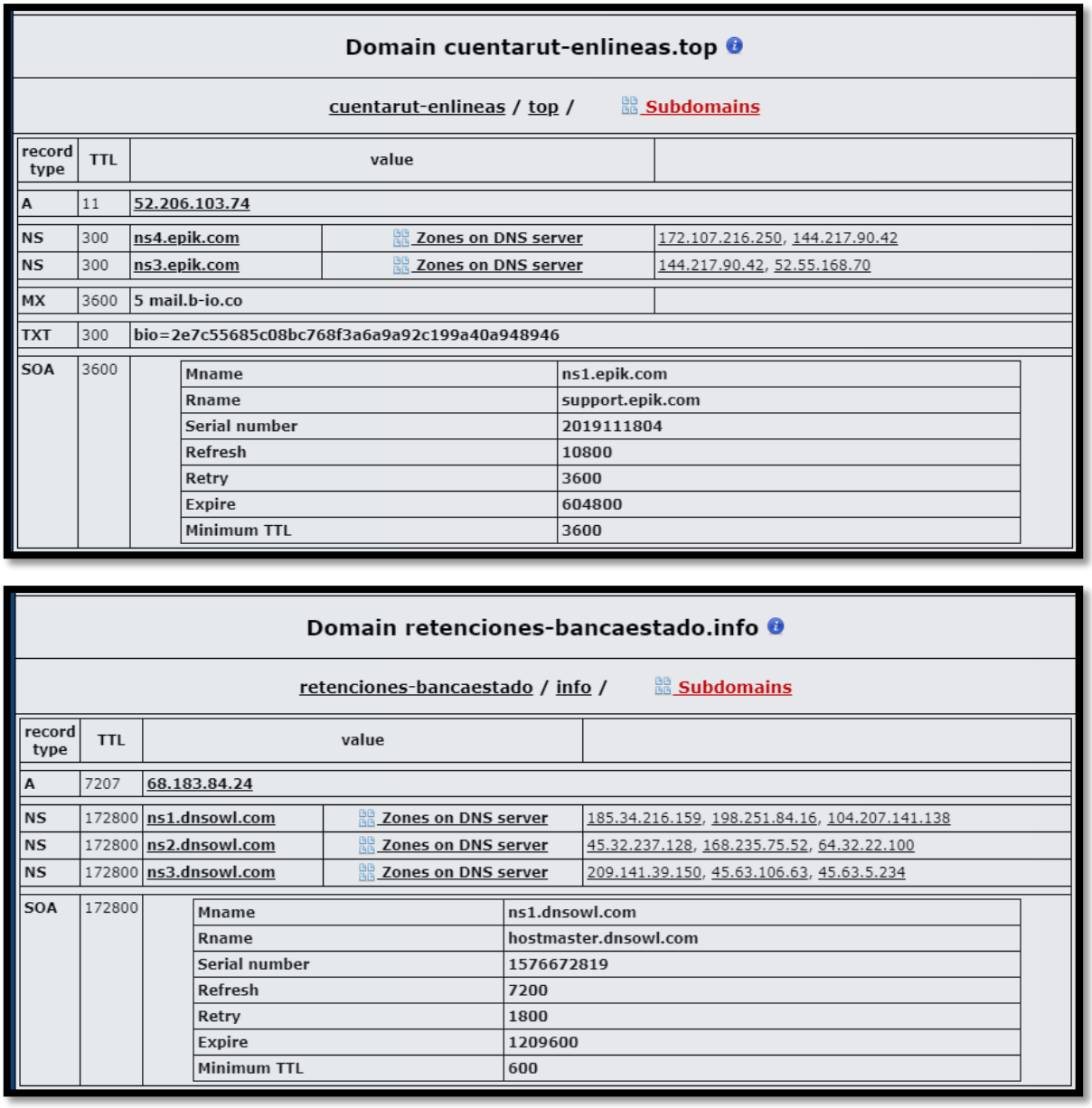
El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de tres portales fraudulentos asociados a una IP que suplantan el sitio web oficial de Banco Estado, el que podría servir para robar credenciales de usuarios de esa entidad.

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

cuentarut-enlineas[.]top/imagenes/comun2008
www[.]retenciones-bancaestado[.]info/
www[.]retenciones-bancaestado[.]info/imagenes/comun2008/banca-en-linea-personas[.]php?html



Domain cuentarut-enlineas.top

cuentarut-enlineas / top / Subdomains

record type	TTL	value		
A	11	52.206.103.74		
NS	300	ns4.epik.com	Zones on DNS server	172.107.216.250, 144.217.90.42
NS	300	ns3.epik.com	Zones on DNS server	144.217.90.42, 52.55.168.70
MX	3600	5 mail.b-io.co		
TXT	300	bio=2e7c55685c08bc768f3a6a9a92c199a40a948946		

SOA	3600	Mname	ns1.epik.com
		Rname	support.epik.com
		Serial number	2019111804
		Refresh	10800
		Retry	3600
		Expire	604800
		Minimum TTL	3600

Domain retenciones-bancaestado.info

retenciones-bancaestado / info / Subdomains

record type	TTL	value		
A	7207	68.183.84.24		
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	45.32.237.128, 168.235.75.52, 64.32.22.100
NS	172800	ns3.dnsowl.com	Zones on DNS server	209.141.39.150, 45.63.106.63, 45.63.5.234

SOA	172800	Mname	ns1.dnsowl.com
		Rname	hostmaster.dnsowl.com
		Serial number	1576672819
		Refresh	7200
		Retry	1800
		Expire	1209600
		Minimum TTL	600

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

Certificados

Subject DN	CN=cuentarut-enlineas.top
Issuer DN	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
Serial	356075889624224201294355235976301664254018
Validity	2019-11-18 21:09:50 **to** 2020-02-16 21:09:50 (90 days, 0:00:00)
Names	cuentarut-enlineas.top

Subject DN	CN=www.retenciones-bancaestado.info
Issuer DN	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
Serial	299153204697042217252490197417690697344088
Validity	2019-12-18 10:22:52 **to** 2020-03-17 10:22:52 (90 days, 0:00:00)
Names	www.retenciones-bancaestado.info

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

IP

52[.]206[.]103[.]74

68[.]183[.]84[.]24

Domain cuentarut-enlineas.top is located on IP address << 52.206.103.74 >>

Block start	52.192.0.0
End of block	52.223.255.255
Block size	2097152 Domains in block
Block name	AT-88-Z
AS number	14618
Parent block	52.119.0.0 - 52.255.255.255
Organization	Amazon Technologies Inc.
City	Ashburn
Region/State	Virginia
Country	US , United States
Reg. date	2015-09-02
Host name	ec2-52-206-103-74.compute-1.amazonaws.com

Domain retenciones-bancaestado.info is located on IP address << 68.183.84.24 >>	
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 retenciones-bancaestado.info

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

Localización

Ashburn, Virginia, Estados Unidos
Bangalore, Karnataka, India

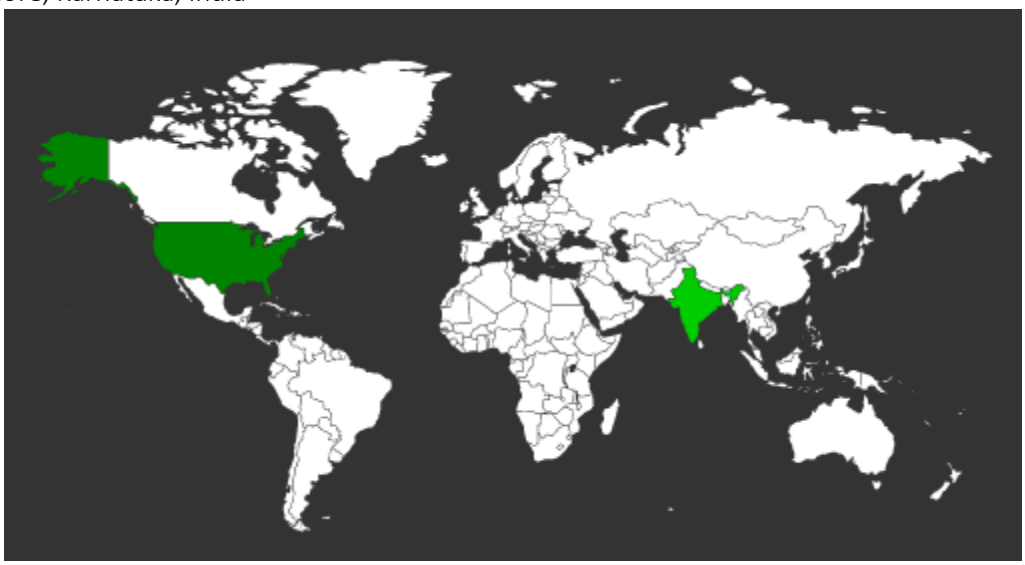
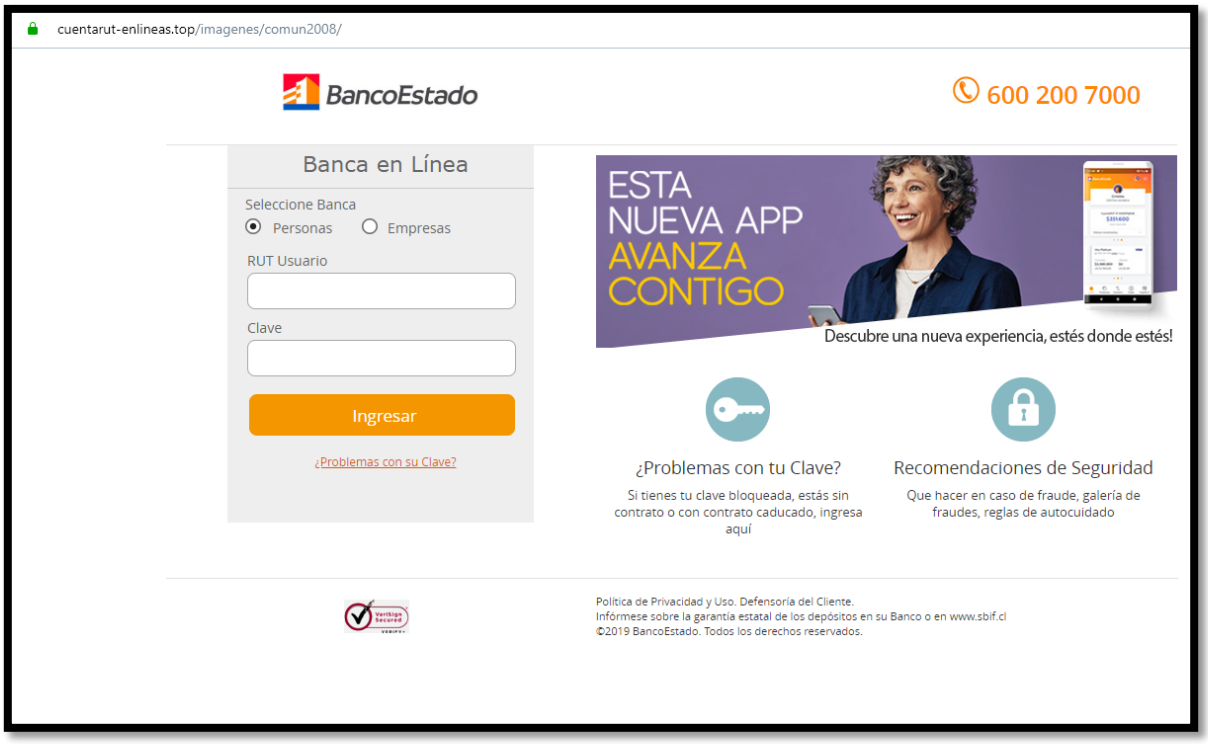
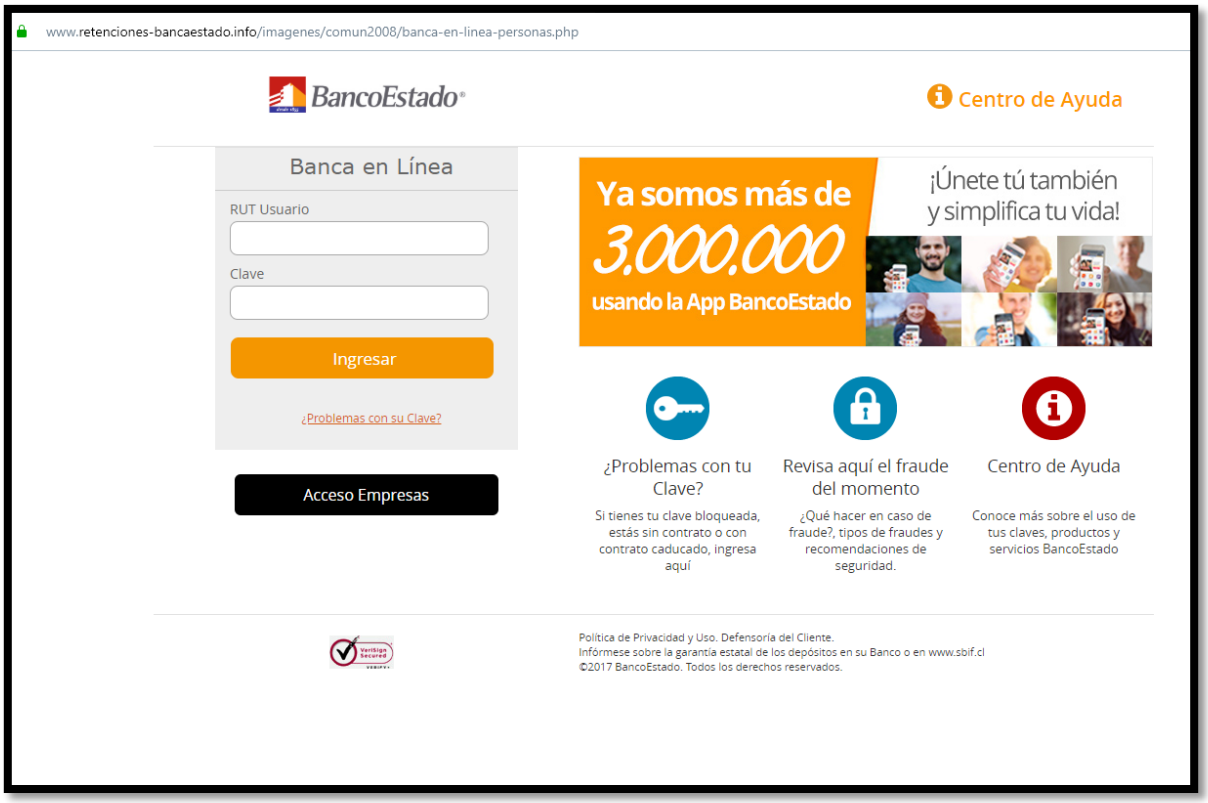


Imagen del sitio





Whois

```
Domain Name: cuentarut-enlineas.top
Registry Domain ID: D20191119G10001G_25940786-top
Registrar WHOIS Server: WHOIS.EPIK.COM
Registrar URL: http://EPIK.COM
Updated Date: 2019-11-18T21:59:23Z
Creation Date: 2019-11-18T21:59:18Z
Registry Expiry Date: 2020-11-18T21:59:18Z
Registrar: EPIK LLC
Registrar IANA ID: 617
Registrar Abuse Contact Email: support@epik.com
Registrar Abuse Contact Phone: +1.4252025160
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Registry Registrant ID: C20191119C_48074605-top
Registrant Name:
Registrant Organization:
Registrant Street:
Registrant City:
Registrant State/Province:
Registrant Postal Code:
Registrant Country:
Registrant Phone:
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email:
Registry Admin ID: C20191119C_48074606-top
Admin Name:
Admin Organization:
Admin Street:
Admin City:
Admin State/Province:
Admin Postal Code:
Admin Country:
Admin Phone:
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email:
Registry Tech ID: C20191119C_48074607-top
Tech Name:
Tech Organization:
Tech Street:
Tech City:
Tech State/Province:
Tech Postal Code:
Tech Country:
Tech Phone:
Tech Phone Ext:
Tech Fax:
Tech Fax Ext:
Tech Email:
Name Server: ns3.epik.com
Name Server: ns4.epik.com
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of WHOIS database: 2019-12-18T19:27:26Z <<<

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

```
Domain Name: retenciones-bancaestado.info
Registrar WHOIS Server: whois.namesilo.com
Registrar URL: https://www.namesilo.com/
Updated Date: 2019-12-18T07:00:00Z
Creation Date: 2019-12-18T07:00:00Z
Registrar Registration Expiration Date: 2020-12-18T07:00:00Z
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-db0f8b8de387e70c6b9d8b56b5fa38c8@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-db0f8b8de387e70c6b9d8b56b5fa38c8@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-db0f8b8de387e70c6b9d8b56b5fa38c8@privacyguardian.org
Name Server: PREMIUM-NS1.DNSOWL.COM
Name Server: PREMIUM-NS2.DNSOWL.COM
Name Server: PREMIUM-NS3.DNSOWL.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: 2019.12.19 17:56:46 -03'00'