Alerta de seguridad cibernética	8FFR20-00437-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	30 de Mayo de 2020
Última revisión	30 de Mayo 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 un portale fraudulento asociado a una IP que suplanta 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 compromiso

URL
bancestado-actualizaciondeinformacion[.]ml

IP
178[.]159[.]36[.]211

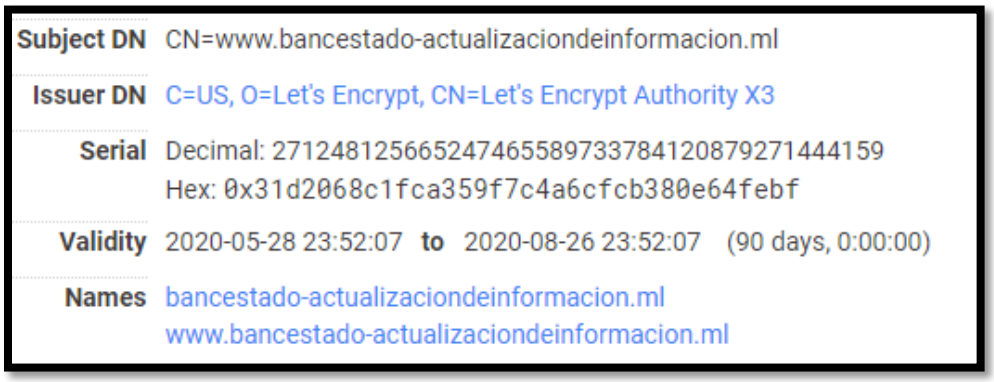
Dominios donde se aloja url

Domain bancestado-actualizaciondeinformacion.ml

bancestado-actualizaciondeinformacion / ml / Subdomains

record type	TTL	value		
A	300	178.159.36.211		
NS	300	ns02.freenom.com	Zones on DNS server	52.19.156.76
NS	300	ns04.freenom.com	Zones on DNS server	104.155.29.241
NS	300	ns03.freenom.com	Zones on DNS server	104.155.27.112
NS	300	ns01.freenom.com	Zones on DNS server	54.171.131.39
SOA	300	Mname	ns01.freenom.com	
		Rname	soa.freenom.com	
		Serial number	1590709182	
		Refresh	10800	
		Retry	3600	
		Expire	604800	
		Minimum TTL	3600	

Certificados



Ip de origen donde se aloja sitio

Domain bancestado-actualizaciondeinformacion.ml is located on IP address << 178.159.36.211 >>

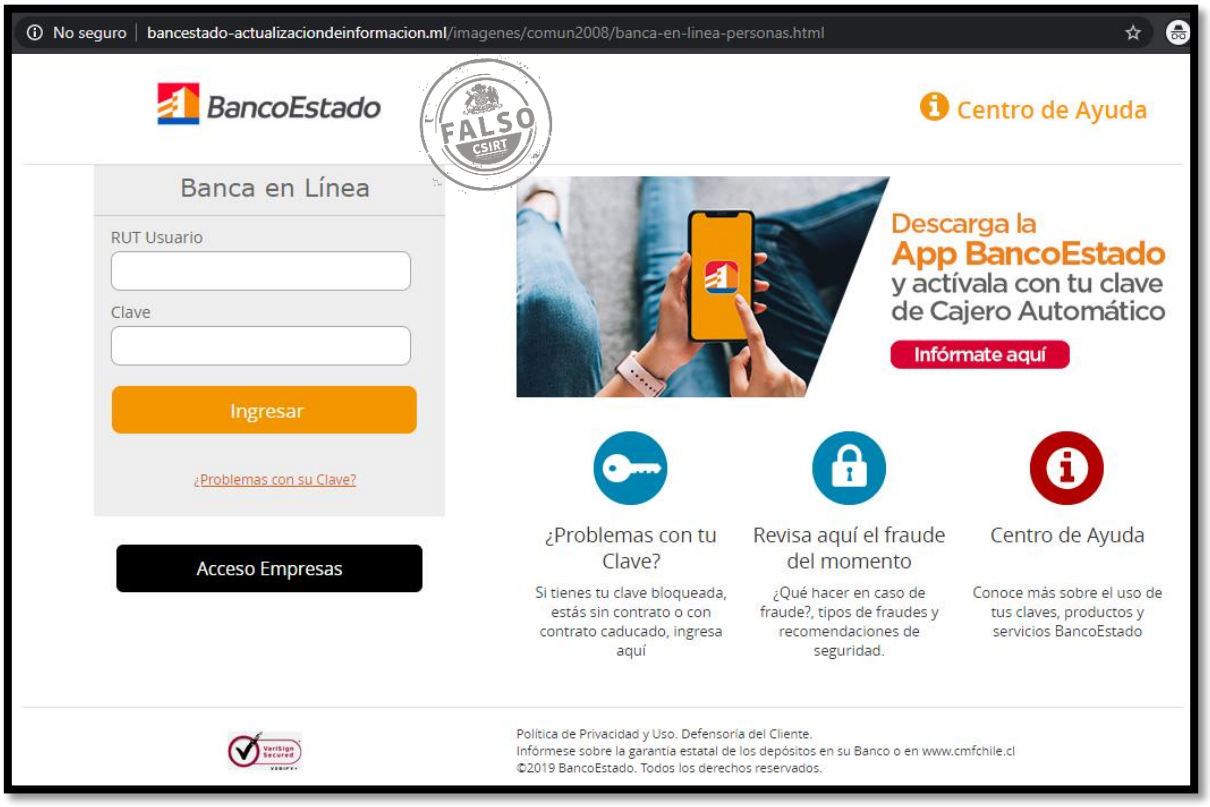
Block start	178.159.36.0
End of block	178.159.36.255
Block size	256 Domains in block
Block name	PrivateInternetHosting
AS number	35196
Parent block	178.0.0.0 - 178.255.255.255
Organization	ORG-PIHL2-RIPE

Localización

Moscú, Federación Rusa

Location	Russia (RU)
Latitude and Longitude	55.74, 37.61

Imagen del sitio



Whois

```
Domain name:
   BANCESTADO-ACTUALIZACIONDEINFORMACION.ML

Organisation:
   Mali Dili B.V.
   Point ML administrator
   P.O. Box 11774
   1001 GT  Amsterdam
   Netherlands
   Phone: +31 20 5315725
   Fax: +31 20 5315721
   E-mail: abuse: abuse@freenom.com, copyright infringement: copyright@freenom.com

Domain Nameservers:
   NS01.FREENOM.COM
   NS02.FREENOM.COM
   NS03.FREENOM.COM
   NS04.FREENOM.COM


Your selected domain name is a Free Domain. That means that,
according to the terms and conditions of Free Domain domain names
the registrant is Mali Dili B.V.

Due to restrictions in Point ML 's Privacy Statement personal information
about the user of the domain name cannot be released.

ABUSE OF A DOMAIN NAME
If you want to report abuse of this domain name, please send a
detailed email with your complaint to abuse@freenom.com.
In most cases Point ML responds to abuse complaints within one business day.

COPYRIGHT INFRINGEMENT
If you want to report a case of copyright infringement, please send
an email to copyright@freenom.com, and include the full name and address of
your organization. Within 5 business days copyright infringement notices
will be investigated.

Record maintained by: Point ML Domain Registry
```

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.