Alerta de seguridad cibernética	8FFR20-00324-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	08 de abril de 2020
Última revisión	08 de abril 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 portal fraudulento asociado a una IP que suplanta el sitio web oficial de la tarjeta Cencosud, 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
tarjetacencosud-activa[.]cf

IP
178[.]159[.]36[.]139

DOMINIOS DONDE SE ALOJA URL

Domain tarjetacencosud-activa.cf

tarjetacencosud-activa / cf / Subdomains

record type	TTL	value		
A	300	178.159.36.139		
NS	300	ns02.freenom.com	Zones on DNS server	52.19.156.76
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
NS	300	ns04.freenom.com	Zones on DNS server	104.155.29.241
SOA	300	Mname	ns01.freenom.com	
		Rname	soa.freenom.com	
		Serial number	1586101709	
		Refresh	10800	
		Retry	3600	
		Expire	604800	
		Minimum TTL	3600	

CERTIFICADOS

Certificates

crt.sh ID	Logged At	Not Before	Not After	Matching Identities	Issuer Name
2670429603	2020-04-05	2020-04-05	2020-07-04	tarjetacencosud-activa.cf www.tarjetacencosud-activa.cf	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
2670429783	2020-04-05	2020-04-05	2020-07-04	tarjetacencosud-activa.cf www.tarjetacencosud-activa.cf	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3

IP DE ORIGEN DONDE SE ALOJA SITIO

Domain tarjetacencosud-activa.cf is located on IP address
<< 178.159.36.139 >>

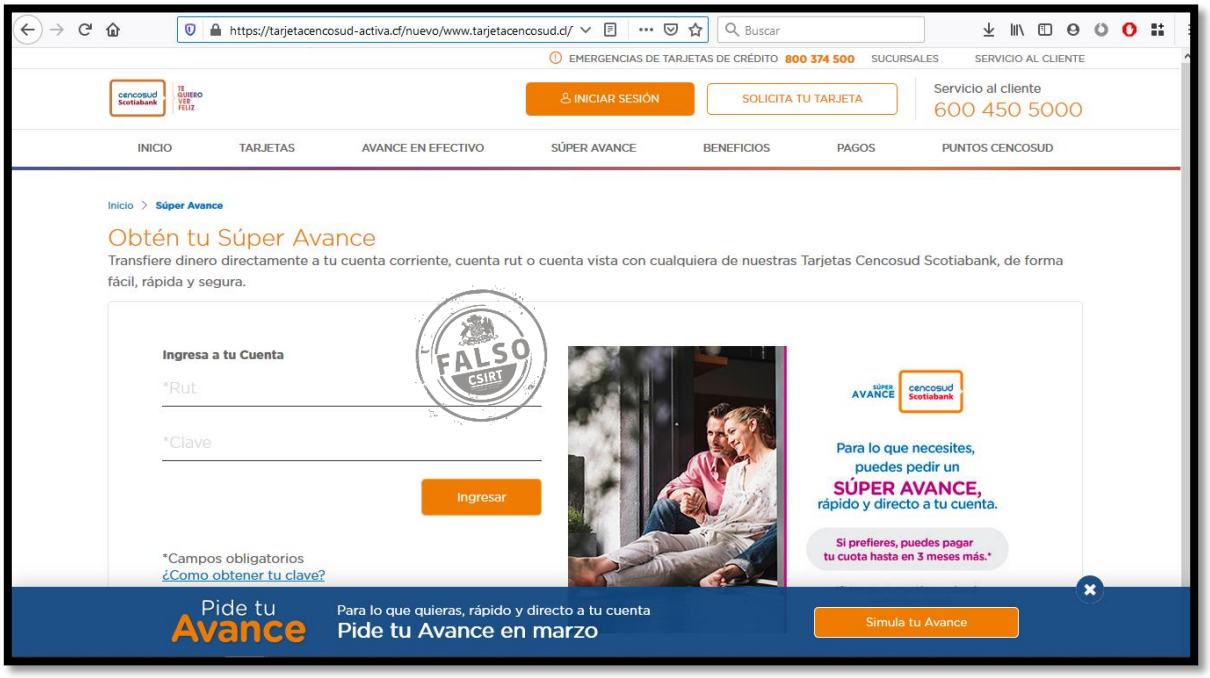
Block start	178.159.36.0
End of block	178.159.36.255
Block size	256 Domains in block
Block name	PrivateInternetHosting
AS number	35196
Parent block	178.0.0.0 - 178.255.255.255
Organization	ORG-PIHL2-RIPE

LOCALIZACIÓN

Moscú, Federación Rusa

Location	Russia (RU)
Latitude and Longitude	55.74, 37.61

IMAGEN DEL SITIO



WHOIS

```
refer:        whois.dot.cf

domain:       CF

organisation: Societe Centrafricaine de Telecommunications (SOCATEL)
address:      Rue guerillot
address:      Bangui  BP 939
address:      Central African Republic

contact:      administrative
name:         Directeur General
organisation: Societe Centrafricaine de Telecommunications (SOCATEL)
address:      Rue guerillot
address:      Bangui  BP 939
address:      Central African Republic
phone:        +236 21 61 60 64
fax-no:       +236 21 61 44 72
e-mail:       dg-socatel@socatel.cf

contact:      technical
name:         Manager ICT
organisation: Centrafrique TLD B.V.
address:      Danzigerkade 23D
address:      Amsterdam
address:      NH  1013 AP
address:      Netherlands
phone:        +31 20 5315726
fax-no:       +31 20 5315721
e-mail:       info@centrafriquetld.com

nserver:      A.NS.CF 185.21.168.17 2a04:1b00:4:0:0:0:0:1
nserver:      B.NS.CF 185.21.169.17 2a04:1b00:5:0:0:0:0:1
nserver:      C.NS.CF 185.21.170.17 2a04:1b00:6:0:0:0:0:1
nserver:      D.NS.CF 185.21.171.17 2a04:1b00:7:0:0:0:0:1

whois:        whois.dot.cf

status:       ACTIVE
remarks:      Registration information: http://www.dot.cf

created:      1996-04-24
changed:      2015-12-29
source:       IANA

WHOIS lookup for TARJETACENCOSUD-ACTIVA.CF can temporarily not be answered. Plea
```

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: 2020.04.08 12:47:10 -04'00'