

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 loC 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 loC 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

tarjetacensosud-activa[.]cf

IP

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

DOMINIOS DONDE SE ALOJA URL

Domain tarjetacensosud-activa.cf ⓘ																	
tarjetacensosud-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	<table border="1"> <tr> <td>Mname</td> <td>ns01.freenom.com</td> </tr> <tr> <td>Rname</td> <td>soa.freenom.com</td> </tr> <tr> <td>Serial number</td> <td>1586101709</td> </tr> <tr> <td>Refresh</td> <td>10800</td> </tr> <tr> <td>Retry</td> <td>3600</td> </tr> <tr> <td>Expire</td> <td>604800</td> </tr> <tr> <td>Minimum TTL</td> <td>3600</td> </tr> </table>		Mname	ns01.freenom.com	Rname	soa.freenom.com	Serial number	1586101709	Refresh	10800	Retry	3600	Expire	604800	Minimum TTL	3600
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	tarjetacensosud-activa.cf www.tarjetacensosud-activa.cf	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	2670429783	2020-04-05	2020-04-05	2020-07-04	tarjetacensosud-activa.cf www.tarjetacensosud-activa.cf	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3

IP DE ORIGEN DONDE SE ALOJA SITIO

Domain <u>tarjetacencosud-activa.cf</u> 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


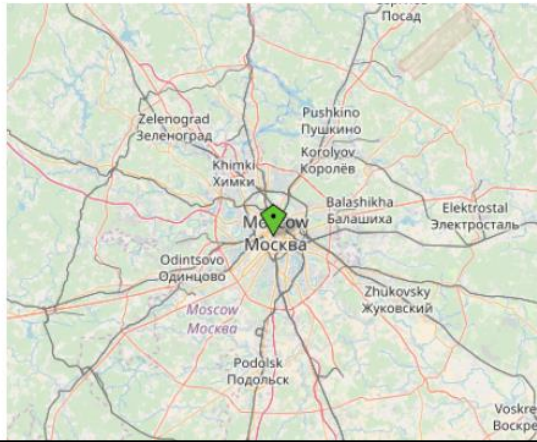
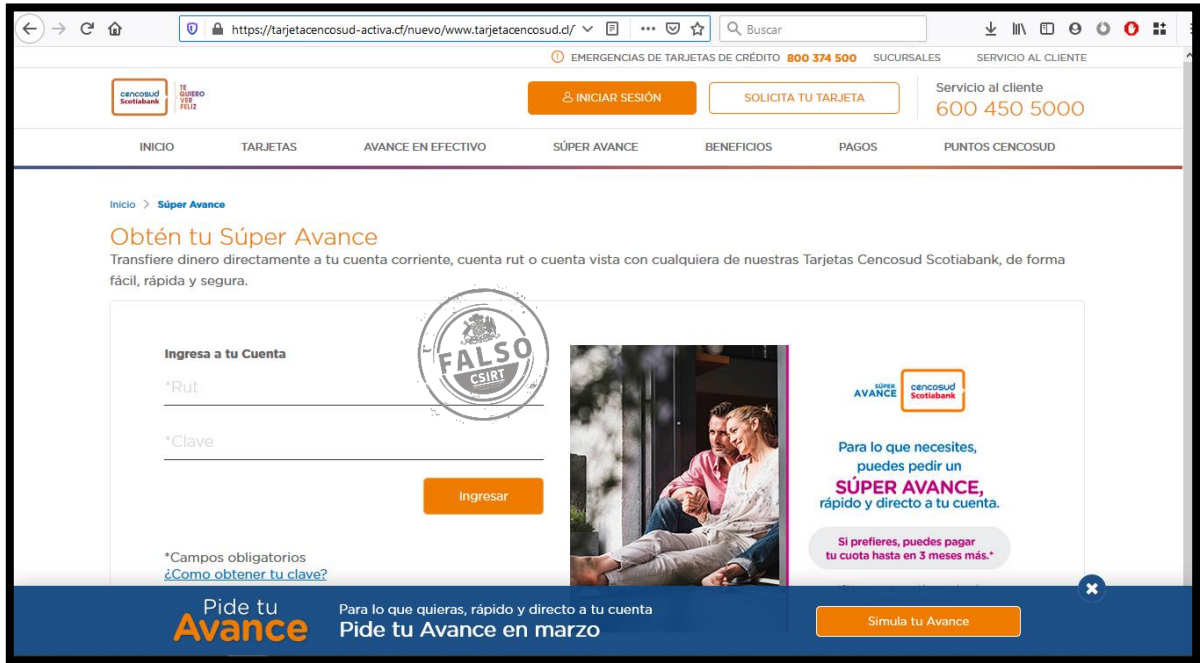
Location	Russia (RU) 
Latitude and Longitude	55.74, 37.61
	

IMAGEN DEL SITIO



The screenshot shows the website interface for Cencosud Scotiabank's 'Súper Avance' service. At the top, there is a navigation bar with the Cencosud Scotiabank logo, a search bar, and links for 'EMERGENCIAS DE TARJETAS DE CRÉDITO 800 374 500', 'SUCURSALES', and 'SERVICIO AL CLIENTE 600 450 5000'. Below this is a menu with options: 'INICIO', 'TARJETAS', 'AVANCE EN EFECTIVO', 'SÚPER AVANCE', 'BENEFICIOS', 'PAGOS', and 'PUNTOS CENCOSUD'. The main content area features a heading 'Obtén tu Súper Avance' and a sub-heading 'Transfiere dinero directamente a tu cuenta corriente, cuenta rut o cuenta vista con cualquiera de nuestras Tarjetas Cencosud Scotiabank, de forma fácil, rápida y segura.' Below this is a login form titled 'Ingresa a tu Cuenta' with fields for '*Rut' and '*Clave', and an 'Ingresar' button. To the right of the form is a circular stamp that says 'FALSO CSIRT'. Further right is a promotional image of a couple sitting together, with text that says 'Para lo que necesitas, puedes pedir un SÚPER AVANCE, rápido y directo a tu cuenta.' and 'Si prefieres, puedes pagar tu cuota hasta en 3 meses más.*'. At the bottom of the page, there is a blue banner with the text 'Pide tu Avance' and 'Para lo que quieras, rápido y directo a tu cuenta Pide tu Avance en marzo', along with a 'Simula tu Avance' button.

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.