Alerta de seguridad informática	8FFR20-00189-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	25 de Enero de 2020
Última revisión	25 de Enero 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 Banco BCI, 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

mfl-rj[.]com[.]br/bcl-emprersas[.]cl/

Domain mfl-rj.com.br

mfl-rj / com / br / Subdomains

record type	TTL	value		
A	14400	187.16.145.180		
NS	86400	dns2.westhost.com.br	Zones on DNS server	187.16.145.135
NS	86400	dns1.westhost.com.br	Zones on DNS server	187.16.145.134
MX	14400	0 mfl-rj.com.br		
TXT	14400	v=spf1 ip4:187.16.145.179 +a +mx ~all		
SOA	86400	Mname	dns1.westhost.com.br	
		Rname	avisoserverhost.west.com.br	
		Serial number	2019092400	
		Refresh	3600	
		Retry	7200	
		Expire	1209600	
		Minimum TTL	86400	

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

Certificados

Basic Information

Subject DN	CN=cpanel.mfl-rj.com.br
Issuer DN	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
Serial	262931651800070706866177782468491117903748
Validity	2020-01-15 02:05:17 **to** 2020-04-14 02:05:17 (90 days, 0:00:00)
Names	cpanel.mfl-rj.com.br mail.mfl-rj.com.br mfl-rj.com.br webdisk.mfl-rj.com.br webmail.mfl-rj.com.br www.mfl-rj.com.br

Ilustración 2 Certificado Utilizado en Url del sitio Falso del Banco BCI

IP

187.16.145.180

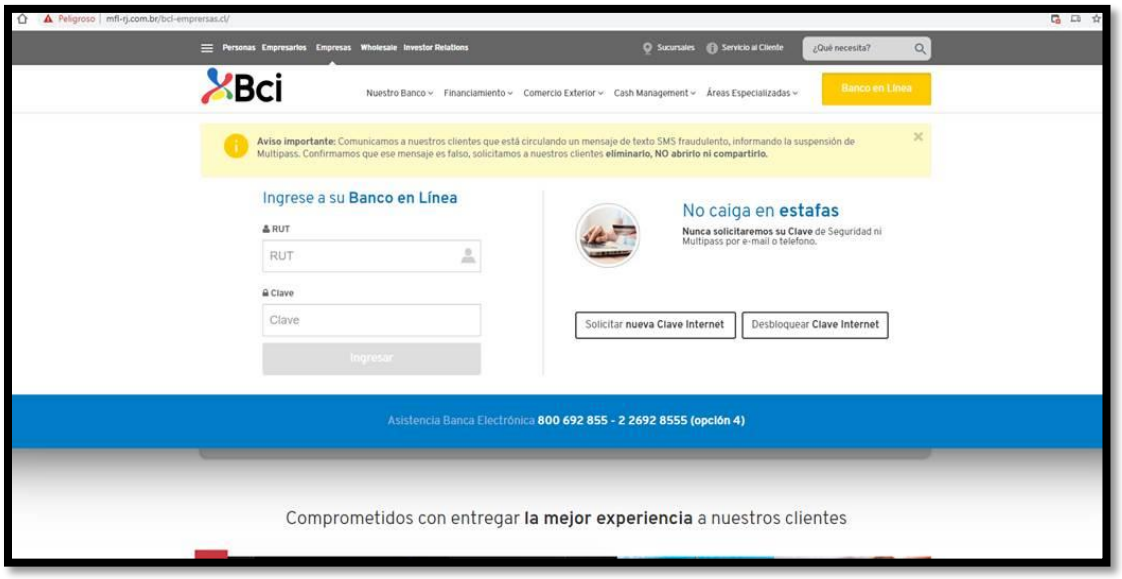
Domain mfl-rj.com.br is located on IP address << 187.16.145.180 >>	
Block start	187.16.144.0
End of block	187.16.159.255
Block size	4096 Domains in block
Block name	
AS number	28255
Parent block	187.0.0.0 - 187.255.255.255
Organization	WEST INTERNET BANDA LARGA
City	Rio de Janeiro
Region/State	Rio de Janeiro
Country	BR , Brazil
Reg. date	2008-09-29
Host name	dell10w.westhost.com.br

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

Localización

Rio de Janeiro, Brasil

Imagen del sitio



Whois

```
% Copyright (c) Nic.br
%  The use of the data below is only permitted as described in
%  full by the terms of use at https://registro.br/termo/en.html ,
%  being prohibited its distribution, commercialization or
%  reproduction, in particular, to use it for advertising or
%  any similar purpose.
%  2020-01-23T12:36:11-03:00

% reserved:     trademark

% Security and mail abuse issues should also be addressed to
% cert.br, http://www.cert.br/ , respectivelly to cert@cert.br
% and mail-abuse@cert.br
%
% whois.registro.br accepts only direct match queries. Types
% of queries are: domain (.br), registrant (tax ID), ticket,
% provider, contact handle (ID), CIDR block, IP and ASN.
```

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: 2020.01.25 12:19:27 -03'00'