Alerta de seguridad informática	8FFR-00118-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	22 de Noviembre de 2019
Última revisión	22 de Noviembre 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 un portal fraudulento asociado a una IP que suplanta el sitio web oficial de **Banco Falabella**, 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

URL Sitio Clonado:
http[://]baciofailabeilla[.]com/home

Domain baciofailabeilla.com				
baciofailabeilla / com / Subdomains				
record type	TTL	value		
A	600	52.15.158.65		
NS	10800	ns3.dongee.com	Zones on DNS server	87.98.146.77
NS	10800	ns2.dongee.com	Zones on DNS server	144.202.22.35
NS	10800	ns1.dongee.com	Zones on DNS server	45.32.171.91
MX	600	0 baciofailabeilla.com		
TXT	600	v=spf1 mx a include:_spf.dongee.com ~all		
SOA	10800	Mname	ns1.dongee.com	
		Rname	root.yei.dongee.com	
		Serial number	2019111502	
		Refresh	3600	
		Retry	1800	
		Expire	1209600	
		Minimum TTL	86400	

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

Certificado

Criteria	Identity = 'baciofailabeilla.com'

Certificates	crt.sh ID	Logged At	Not Before	Not After	Issuer Name
	2117474904	2019-11-16	2019-11-16	2020-02-14	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	2117475018	2019-11-16	2019-11-16	2020-02-14	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3

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

IP

52.15.158.65

Domain baciofailabeilla.com is located on IP address << 52.15.158.65 >>	
Block start	52.0.0.0
End of block	52.31.255.255
Block size	2097152 Domains in block
Block name	AT-88-Z
AS number	16509
Parent block	52.0.0.0 - 52.255.255.255
Organization	Amazon Technologies Inc.
City	Columbus
Region/State	Ohio
Country	US , United States
Reg. date	1991-12-19
Host name	ec2-52-15-158-65.us-east-2.compute.amazonaws.com
Domains	1 baciofailabeilla.com

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

Localización

Columbia, Ohio, Estados Unidos

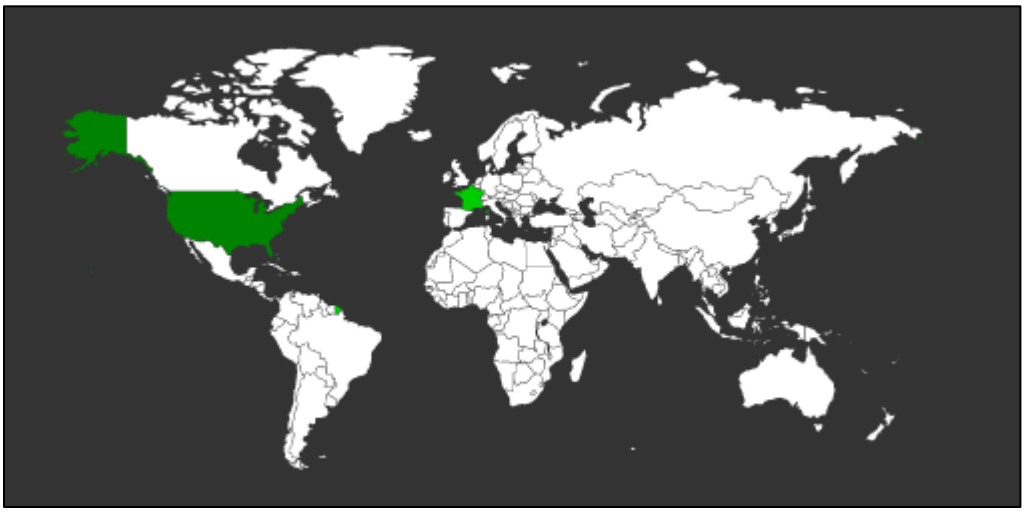
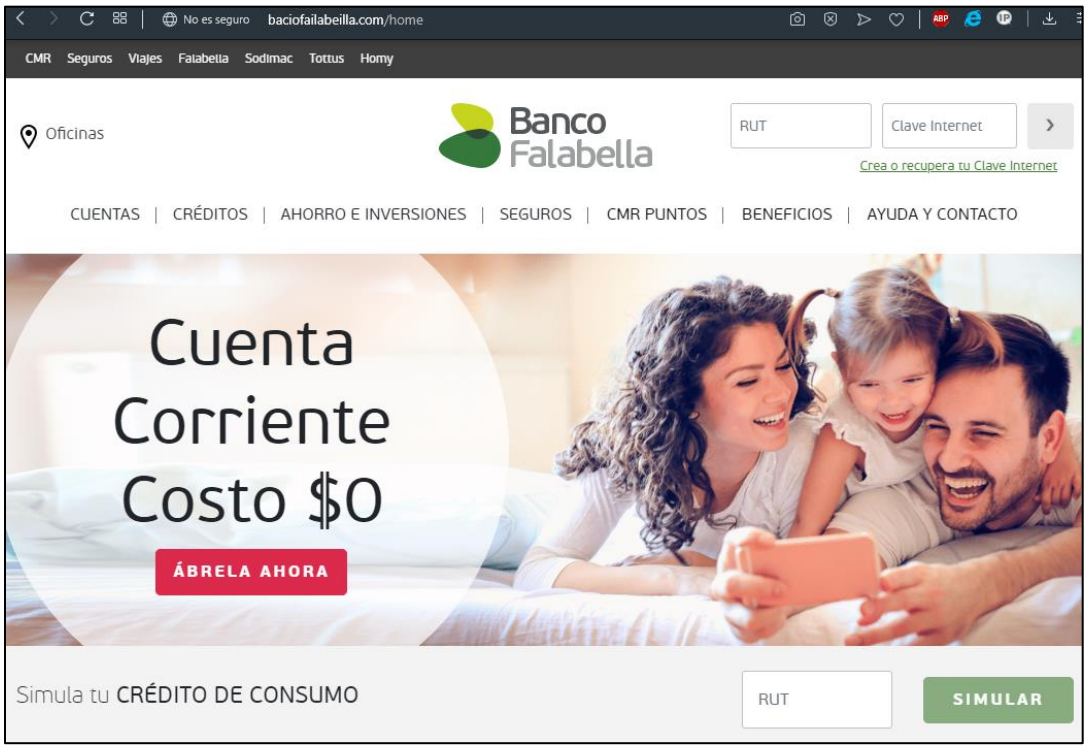


Imagen del sitio



Whois

```
Domain Name: baciofailabeilla.com
Registry Domain ID: 2455575509_DOMAIN_COM-VRSN
Registrar WHOIS Server: WHOIS.ENOM.COM
Registrar URL: WWW.ENOM.COM
Updated Date: 2019-11-15T19:01:47.00Z
Creation Date: 2019-11-15T19:01:00.00Z
Registrar Registration Expiration Date: 2020-11-15T19:01:00.00Z
Registrar: ENOM, INC.
Registrar IANA ID: 48
Domain Status: clientTransferProhibited https://www.icann.org/epp#clientTransferProhibited
Domain Status: addPeriod https://www.icann.org/epp#addPeriod
Registrant Name: REDACTED FOR PRIVACY
Registrant Organization: REDACTED FOR PRIVACY
Registrant Street: REDACTED FOR PRIVACY
Registrant Street:
Registrant City: REDACTED FOR PRIVACY
Registrant State/Province: region metropolitana
Registrant Postal Code: REDACTED FOR PRIVACY
Registrant Country: CL
Registrant Phone: REDACTED FOR PRIVACY
Registrant Phone Ext:
Registrant Fax: REDACTED FOR PRIVACY
Registrant Email: https://tieredaccess.com/contact/d352ec11-c7dd-41a7-b11a-b25883faba79
Admin Name: REDACTED FOR PRIVACY
Admin Organization: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
Admin Street:
Admin City: REDACTED FOR PRIVACY
Admin State/Province: REDACTED FOR PRIVACY
Admin Postal Code: REDACTED FOR PRIVACY
Admin Country: REDACTED FOR PRIVACY
Admin Phone: REDACTED FOR PRIVACY
Admin Phone Ext:
Admin Fax: REDACTED FOR PRIVACY
Admin Email: REDACTED FOR PRIVACY
Tech Name: REDACTED FOR PRIVACY
Tech Organization: REDACTED FOR PRIVACY
Tech Street: REDACTED FOR PRIVACY
Tech Street:
Tech City: REDACTED FOR PRIVACY
Tech State/Province: REDACTED FOR PRIVACY
Tech Postal Code: REDACTED FOR PRIVACY
Tech Country: REDACTED FOR PRIVACY
Tech Phone: REDACTED FOR PRIVACY
Tech Phone Ext:
Tech Fax: REDACTED FOR PRIVACY
Tech Email: REDACTED FOR PRIVACY
Name Server: NS1.DONGEE.COM
Name Server: NS2.DONGEE.COM
Name Server: NS3.DONGEE.COM
DNSSEC: unsigned
Registrar Abuse Contact Email: ABUSE@ENOM.COM
Registrar Abuse Contact Phone: +1.4259744689
URL of the ICANN WHOIS Data Problem Reporting System: HTTP://WDPRS.INTERNIC.NET/
>>> Last update of WHOIS database: 2019-11-18T13:29:53.00Z <<<
```

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: 2019.11.22 10:38:59 -03'00'