Alerta de seguridad informática	8FFR-00170-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	31 de diciembre de 2019
Última revisión	31 de diciembre 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 un portal fraudulento asociado a una IP que ha sido utilizada para suplantar el sitio web oficial del **Banco Falabella**, con el propósito de robar credenciales de usuarios de esa entidad u otras acciones maliciosas.

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
http[://]falebellia[.]com/

Domain falebellia.com

falebellia / com / Subdomains

record type	TTL	value		
A	300	142.11.239.218		
NS	300	ns4dfh.name.com	Zones on DNS server	162.88.60.49
NS	300	ns2cqs.name.com	Zones on DNS server	162.88.60.47
NS	300	ns1stv.name.com	Zones on DNS server	162.88.61.47
NS	300	ns3gnv.name.com	Zones on DNS server	162.88.61.49
SOA	300	Mname	ns1stv.name.com	
		Rname	support.name.com	
		Serial number	1577689812	
		Refresh	10800	
		Retry	3600	
		Expire	604800	
		Minimum TTL	3600	

Ilustración 1 Dominio donde se Aloja Url de BANCO FALABELLA, Falso y DNS que utiliza

Certificados

Subject DN CN=falebellia.com

Issuer DN C=US, ST=TX, L=Houston, O=cPanel, Inc., CN=cPanel, Inc. Certification Authority

Serial 306945172648110997389576884789284491364

Validity 2019-12-30 00:00:00 **to** 2020-03-29 23:59:59 (90 days, 23:59:59)

Names cpanel.falebellia.com
falebellia.com
mail.falebellia.com
webdisk.falebellia.com
webmail.falebellia.com
www.falebellia.com

Ilustración 2 Certificado Utilizado en Url del sitio Falso de BANCO FALABELLA

IP

142[.]11[.]239[.]218

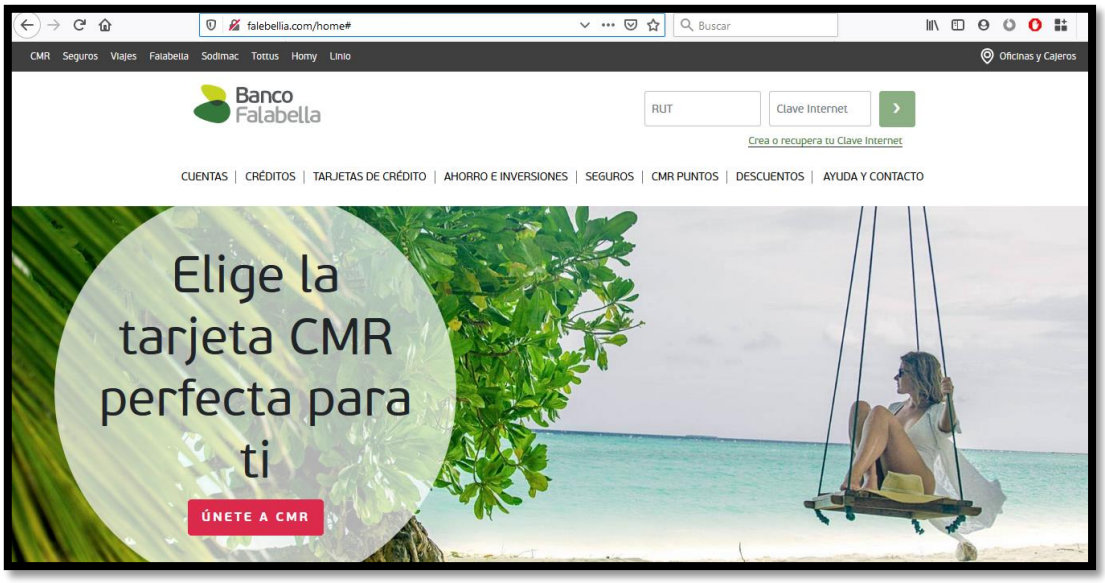
Domain falebellia.com is located on IP address << 142.11.239.218 >>	
Block start	142.11.192.0
End of block	142.11.255.255
Block size	16384 Domains in block
Block name	HOSTWINDS-18-1
AS number	54290
Parent block	142.0.0.0 - 142.255.255.255
Organization	HostwindsLLC.
City	Seattle
Region/State	Washington
Country	US , United States
Reg. date	2012-06-22
Host name	client-142-11-239-218.hostwindsdns.com
Domains	1 falebellia.com

Ilustración 3 Ip de Origen donde se aloja Sitio Falso de BANCO FALABELLA

Localización

Seattle, Washington, Estados Unidos

Imagen del sitio



Whois

```
Domain Name: FALEBELLIA.COM
Registry Domain ID: 2473735363_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.name.com
Registrar URL: http://www.name.com
Updated Date: 2019-12-30T05:15:40Z
Creation Date: 2019-12-30T05:15:39Z
Registrar Registration Expiration Date: 2020-12-30T05:15:39Z
Registrar: Name.com, Inc.
Registrar IANA ID: 625
Reseller:
Domain Status: addPeriod https://www.icann.org/epp#addPeriod
Domain Status: clientTransferProhibited https://www.icann.org/epp#clientTransferProhibited
Registry Registrant ID: Not Available From Registry
Registrant Name: Whois Agent
Registrant Organization: Domain Protection Services, Inc.
Registrant Street: PO Box 1769
Registrant City: Denver
Registrant State/Province: CO
Registrant Postal Code: 80201
Registrant Country: US
Registrant Phone: +1.7208009072
Registrant Fax: +1.7209758725
Registrant Email: https://www.name.com/contact-domain-whois/falebellia.com
Registry Admin ID: Not Available From Registry
Admin Name: Whois Agent
Admin Organization: Domain Protection Services, Inc.
Admin Street: PO Box 1769
Admin City: Denver
Admin State/Province: CO
Admin Postal Code: 80201
Admin Country: US
Admin Phone: +1.7208009072
Admin Fax: +1.7209758725
Admin Email: https://www.name.com/contact-domain-whois/falebellia.com
Registry Tech ID: Not Available From Registry
Tech Name: Whois Agent
Tech Organization: Domain Protection Services, Inc.
Tech Street: PO Box 1769
Tech City: Denver
Tech State/Province: CO
Tech Postal Code: 80201
Tech Country: US
Tech Phone: +1.7208009072
Tech Fax: +1.7209758725
Tech Email: https://www.name.com/contact-domain-whois/falebellia.com
Name Server: nslstv.name.com
Name Server: ns2cqs.name.com
Name Server: ns3gnv.name.com
Name Server: ns4dfh.name.com
DNSSEC: unSigned
```

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: 2019.12.31 12:14:58 -03'00'