Alerta de seguridad cibernética	8FFR20-00298-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	01 de Abril de 2020
Última revisión	01 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 dos portales fraudulentos asociados a dos IPs que suplantan 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 COMPROMISO

URL

falabellacl[.]com
fala-registrarse[.]net
fala-registrarse[.]net/d/

IP

104[.]24[.]103[.]189
104[.]24[.]102[.]189
104[.]27[.]156[.]187
104[.]27[.]157[.]187

DOMINIOS DONDE SE ALOJA URL

Domain falabellacl.com

falabellacl / com / Subdomains

record type	TTL	value		
A	300	104.24.102.189		
A	300	104.24.103.189		
NS	86400	barbara.ns.cloudflare.com	Zones on DNS server	173.245.58.248
NS	86400	cody.ns.cloudflare.com	Zones on DNS server	173.245.59.107

SOA	3600	Mname	barbara.ns.cloudflare.com
		Rname	dns.cloudflare.com
		Serial number	2033725979
		Refresh	10000
		Retry	2400
		Expire	604800
		Minimum TTL	3600

Domain fala-registrarse.net

fala-registrarse / net / Subdomains

record type	TTL	value		
A	300	104.27.156.187		
A	300	104.27.157.187		
NS	86400	shubhi.ns.cloudflare.com	Zones on DNS server	162.159.38.63
NS	86400	terin.ns.cloudflare.com	Zones on DNS server	173.245.59.236

SOA	3600	Mname	shubhi.ns.cloudflare.com
		Rname	dns.cloudflare.com
		Serial number	2033732511
		Refresh	10000
		Retry	2400
		Expire	604800
		Minimum TTL	3600

CERTIFICADOS

Emitido para: sni.cloudflaressl.com

Emitido por: CloudFlare Inc ECC CA-2

Válido desde 29-03-2020 **hasta** 09-10-2020

crt.sh ID	Logged At	Not Before	Not After	Matching Identities	Issuer Name
2648291949	2020-03-31	2020-03-31	2020-10-09	*.fala-registrarse.net fala-registrarse.net	C=US, ST=CA, L=San Francisco, O="CloudFlare, Inc.", CN=CloudFlare Inc ECC CA-2

IP DE ORIGEN DONDE SE ALOJA SITIO

Domain falabellacl.com is located on IP address << 104.24.103.189 >>

Block start	104.16.0.0
End of block	104.31.255.255
Block size	1048576 Domains in block
Block name	CLOUDFLARENET
AS number	13335
Parent block	104.0.0.0 - 104.255.255.255
Organization	CloudFlare, Inc.

Domain falabellacl.com is located on IP address << 104.24.102.189 >>

Block start	104.16.0.0
End of block	104.31.255.255
Block size	1048576 Domains in block
Block name	CLOUDFLARENET
AS number	13335
Parent block	104.0.0.0 - 104.255.255.255
Organization	CloudFlare, Inc.

Domain fala-registrarse.net is located on IP address << 104.27.156.187 >>

Block start	104.16.0.0
End of block	104.31.255.255
Block size	1048576 Domains in block
Block name	CLOUDFLARENET
AS number	13335
Parent block	104.0.0.0 - 104.255.255.255
Organization	CloudFlare, Inc.

Domain fala-registrarse.net is located on IP address << 104.27.157.187 >>

Block start	104.16.0.0
End of block	104.31.255.255
Block size	1048576 Domains in block
Block name	CLOUDFLARENET
AS number	13335
Parent block	104.0.0.0 - 104.255.255.255
Organization	CloudFlare, Inc.

LOCALIZACIÓN

San Francisco, California, Estados Unidos

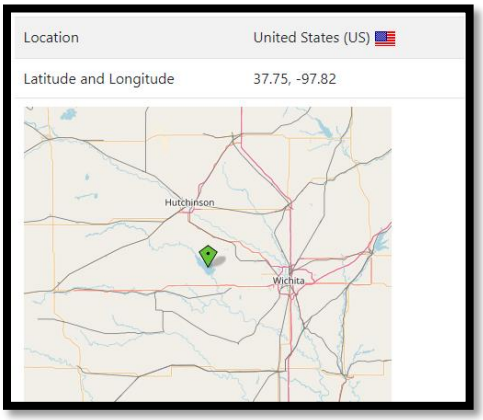
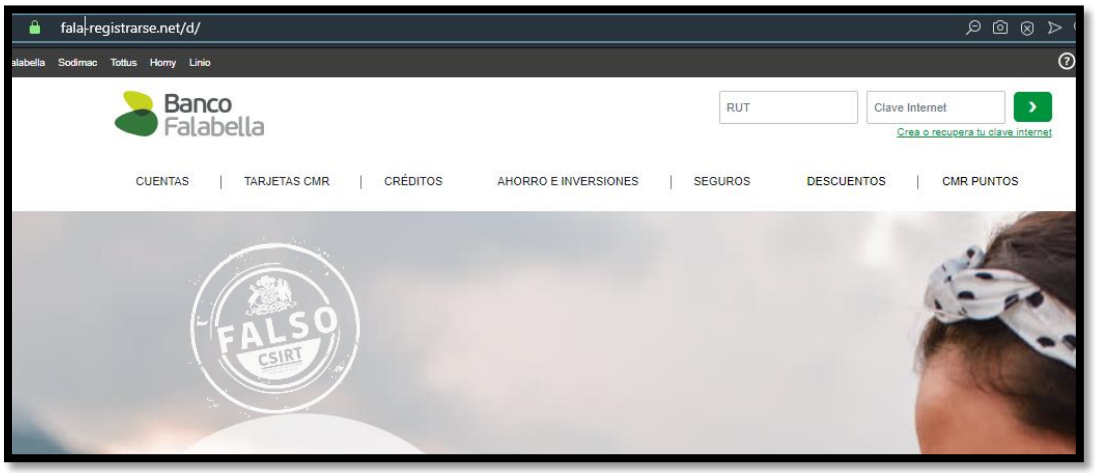


IMAGEN DEL SITIO



WHOIS

```
Domain Name: FALA-REGISTRARSE.NET
Registry Domain ID: 2502194542_DOMAIN_NET-VRSN
Registrar WHOIS Server: whois.ilovewww.com
Registrar URL: http://www.ilovewww.com
Updated Date: 2020-03-11T01:42:41Z
Creation Date: 2020-03-11T01:42:40Z
Registrar Registration Expiration Date: 2021-03-11T01:42:40Z
Registrar: Shinjiru MSC Sdn Bhd
Registrar IANA ID: 1741
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Registry Registrant ID: Not Available From Registry
Registrant Name: Domain Admin
Registrant Organization: Privacy Protect, LLC (PrivacyProtect.org)
Registrant Street: 10 Corporate Drive
Registrant City: Burlington
Registrant State/Province: MA
Registrant Postal Code: 01803
Registrant Country: US
Registrant Phone: +1.8022274003
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: contact@privacyprotect.org
Registry Admin ID: Not Available From Registry
Admin Name: Domain Admin
Admin Organization: Privacy Protect, LLC (PrivacyProtect.org)
Admin Street: 10 Corporate Drive
Admin City: Burlington
Admin State/Province: MA
Admin Postal Code: 01803
Admin Country: US
Admin Phone: +1.8022274003
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: contact@privacyprotect.org
Registry Tech ID: Not Available From Registry
Tech Name: Domain Admin
Tech Organization: Privacy Protect, LLC (PrivacyProtect.org)
Tech Street: 10 Corporate Drive
Tech City: Burlington
Tech State/Province: MA
Tech Postal Code: 01803
Tech Country: US
Tech Phone: +1.8022274003
Tech Phone Ext:
Tech Fax:
Tech Fax Ext:
Tech Email: contact@privacyprotect.org
Name Server: shubhi.ns.cloudflare.com
Name Server: terin.ns.cloudflare.com
DNSSEC: Unsigned
Registrar Abuse Contact Email: abuse@ilovewww.com
Registrar Abuse Contact Phone: +603 2031 8850
```

```
Domain Name: FALABELLACL.COM
Registry Domain ID: 2508998126_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.PublicDomainRegistry.com
Registrar URL: http://www.publicdomainregistry.com
Updated Date: 2020-03-30T18:17:49Z
Creation Date: 2020-03-29T23:44:35Z
Registry Expiry Date: 2021-03-29T23:44:35Z
Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com
Registrar IANA ID: 303
Registrar Abuse Contact Email: abuse-contact@publicdomainregistry.com
Registrar Abuse Contact Phone: +1.2013775952
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Name Server: BARBARA.NS.CLOUDFLARE.COM
Name Server: CODY.NS.CLOUDFLARE.COM
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
```

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: 2020.04.01 13:34:51 -03'00'