Alerta de seguridad cibernética	8FFR20-00291-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	27 de Marzo de 2020
Última revisión	27 de Marzo 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
www[.]falabellaenlinea[.]xyz
IP
190[.]107[.]177[.]238

URL
www[.]falabellacmrchile[.]com
www[.]falabellacmrchile[.]com/site/choose[.]php
www[.]falabellacmrchile[.]com/site/mobile/acesso[.]php
www[.]falabellacmrchile[.]com/site/empresa/acesso[.]php
IP
80[.]211[.]130[.]144

DOMINIOS DONDE SE ALOJA URL

Domain falabellaenlinea.xyz

falabellaenlinea / xyz / Subdomains

record type	TTL	value		
A	14400	190.107.177.238		
NS	86400	ns2.cphost.cl	Zones on DNS server	190.107.177.12
NS	86400	ns1.cphost.cl	Zones on DNS server	190.107.177.11
MX	14400	0 mail.falabellaenlinea.xyz		
TXT	14400	v=spf1 +a +mx +ip4:190.107.177.238 +ip4:200.63.101.158 ~all		

SOA	86400	Mname	ns1.cphost.cl
		Rname	ventas.cpanelhost.cl
		Serial number	2020032503
		Refresh	3600
		Retry	7200
		Expire	1209600
		Minimum TTL	86400

Domain falabellacmrchile.com

falabellacmrchile / com / Subdomains

record type	TTL	value		
A	3600	80.211.130.144		
NS	21600	ns-cloud-e1.googledomains.com	Zones on DNS server	216.239.32.110
NS	21600	ns-cloud-e2.googledomains.com	Zones on DNS server	216.239.34.110
NS	21600	ns-cloud-e3.googledomains.com	Zones on DNS server	216.239.36.110
NS	21600	ns-cloud-e4.googledomains.com	Zones on DNS server	216.239.38.110

SOA	21600	Mname	ns-cloud-e1.googledomains.com
		Rname	cloud-dns-hostmaster.google.com
		Serial number	4
		Refresh	21600
		Retry	3600
		Expire	259200
		Minimum TTL	300

CERTIFICADOS

Certificates

crt.sh ID	Logged At	Not Before	Not After	Matching Identities	Issuer Name
2626920867	2020-03-26	2020-03-26	2020-06-24	cpanel.falabellaenlinea.xyz falabellaenlinea.xyz mail.falabellaenlinea.xyz webdisk.falabellaenlinea.xyz webmail.falabellaenlinea.xyz www.falabellaenlinea.xyz	C=US, ST=TX, L=Houston, O="cPanel, Inc.", CN="cPanel, Inc. Certification Authority"
2626920848	2020-03-26	2020-03-26	2020-06-24	cpanel.falabellaenlinea.xyz falabellaenlinea.xyz mail.falabellaenlinea.xyz webdisk.falabellaenlinea.xyz webmail.falabellaenlinea.xyz www.falabellaenlinea.xyz	C=US, ST=TX, L=Houston, O="cPanel, Inc.", CN="cPanel, Inc. Certification Authority"

Certificates

crt.sh ID	Logged At	Not Before	Not After	Matching Identities	Issuer Name
2631562770	2020-03-26	2020-03-26	2020-06-24	www.falabellacmrchile.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
2630005063	2020-03-26	2020-03-26	2020-06-24	www.falabellacmrchile.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3

IP DE ORIGEN DONDE SE ALOJA SITIO

Domain www.falabellaenlinea.xyz is located on IP address << 190.107.177.238 >>

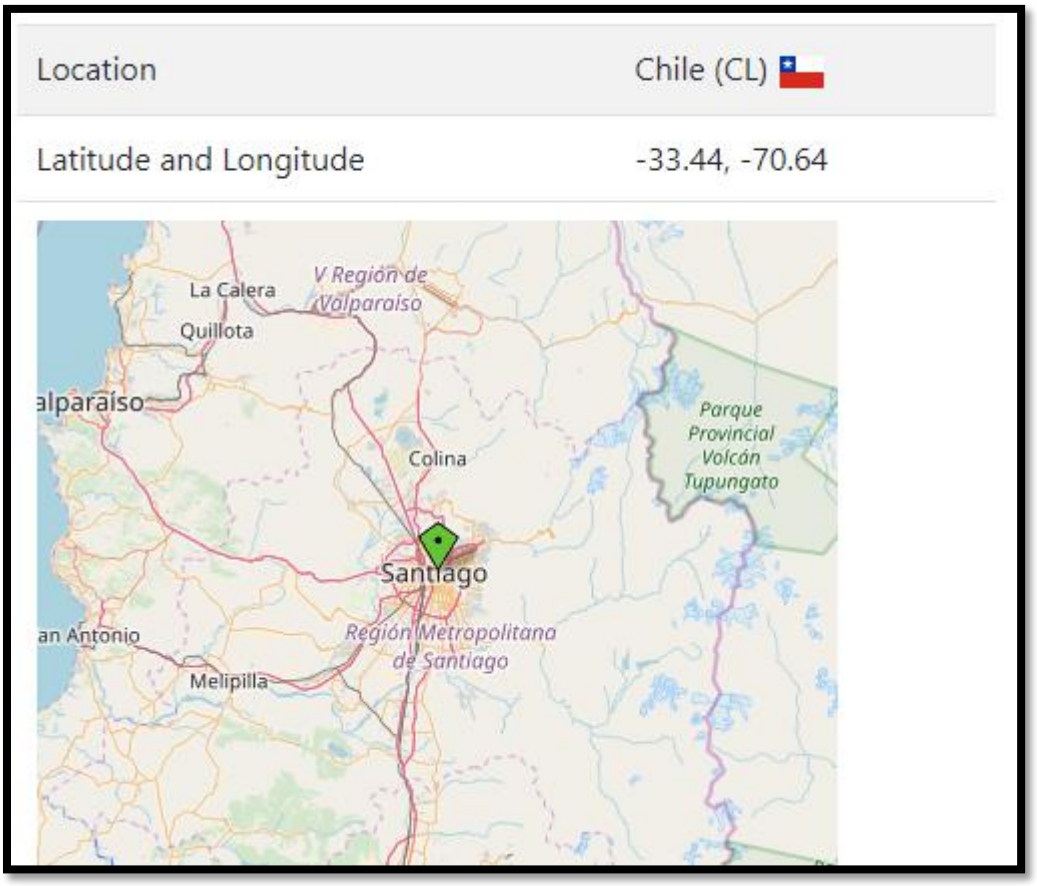
Block start	190.107.176.0
End of block	190.107.179.255
Block size	1024 Domains in block
Block name	
AS number	265831
Parent block	190.0.0.0 - 190.255.255.255
Organization	SOC. COMERCIAL WIRENET CHILE LTDA.

Domain falabellacmrchile.com is located on IP address << 80.211.130.144 >>

Block start	80.211.130.0
End of block	80.211.130.255
Block size	256 Domains in block
Block name	ARUBA-NET
AS number	31034
Parent block	80.211.128.0 - 80.211.191.255
Organization	Aruba S.p.A. - Cloud Services Farm2

LOCALIZACIÓN

Chile, Region Metropolitana, Santiago.



Arezzo, Tuscany, Italia.

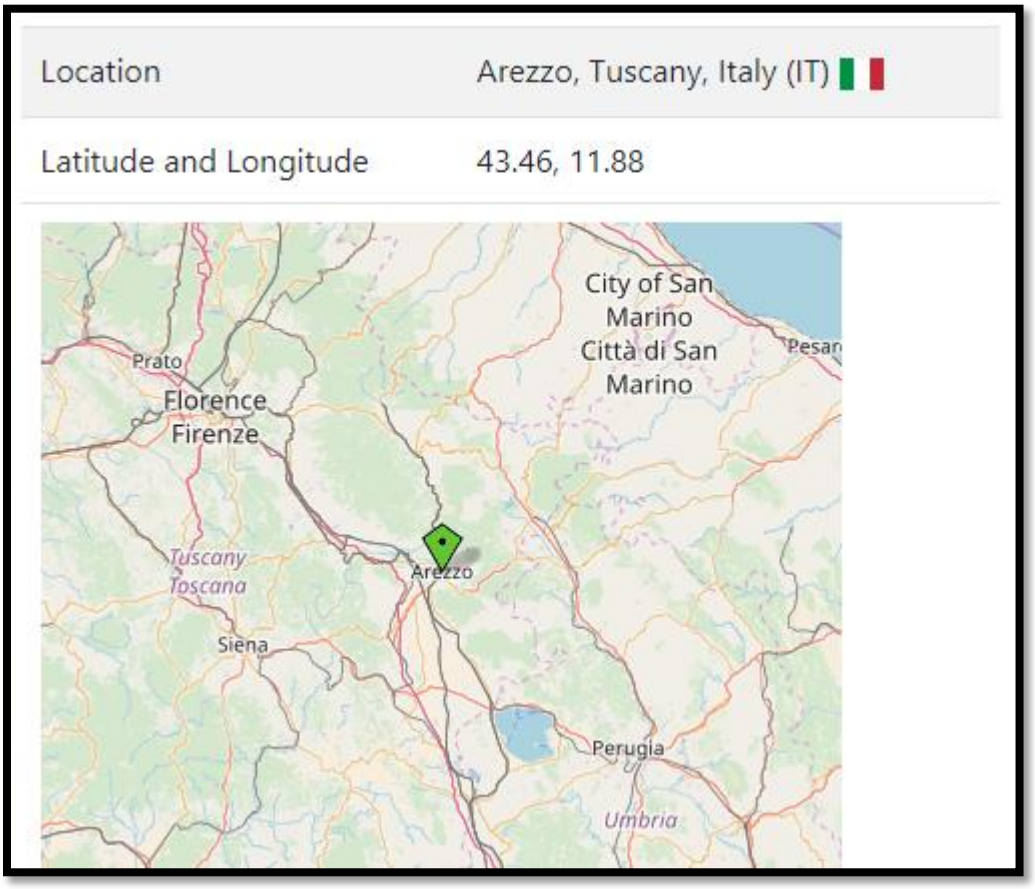


IMAGEN DEL SITIO


www.falabellacmrchile.com/site/choose.php
FALSO
CSIRT
Banco Falabella
Acceda a su banco.
Seleccione el tipo de acceso que desea realizar.
Ingreso Personas
Ingreso Empresas

WHOIS

```
Domain name: falabellaenlinea.xyz
Registry Domain ID: D180084489-CNIC
Registrar WHOIS Server: whois.namecheap.com
Registrar URL: http://www.namecheap.com
Updated Date: 0001-01-01T00:00:00.00Z
Creation Date: 2020-03-25T20:19:35.00Z
Registrar Registration Expiration Date: 2021-03-25T20:19:35.
Registrar: NAMECHEAP INC
Registrar IANA ID: 1068
Registrar Abuse Contact Email: abuse@namecheap.com
Registrar Abuse Contact Phone: +1.6613102107
Reseller: NAMECHEAP INC
```

```
Domain Name: falabellacmrchile.com
Registry Domain ID: 2507608663_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.google.com
Registrar URL: https://domains.google.com
Updated Date: 2020-03-26T14:38:12Z
Creation Date: 2020-03-26T14:38:11Z
Registrar Registration Expiration Date: 2021-03-26T14:38:11Z
Registrar: Google LLC
Registrar IANA ID: 895
Registrar Abuse Contact Email: registrar-abuse@google.com
Registrar Abuse Contact Phone: +1.8772376466
```

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: 2020.03.27 22:13:11 -03'00'