Alerta de seguridad cibernética	8FFR20-00326-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	09 de abril de 2020
Última revisión	09 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

falabella[.]chilemobile[.]net
falabellacmr[.]chilemobile[.]net
falabellabanco[.]com

IP
212[.]237[.]63[.]113
144[.]208[.]127[.]93

DOMINIOS DONDE SE ALOJA URL

Domain falabella.chilemobile.net

falabella / chilemobile / net / Subdomains

record type	TTL	value
A	3600	212.237.63.113

Domain chilemobile.net

chilemobile / net / Subdomains

record type	TTL	value		
NS	21600	ns-cloud-a1.googledomains.com	Zones on DNS server	216.239.32.106
NS	21600	ns-cloud-a2.googledomains.com	Zones on DNS server	216.239.34.106
NS	21600	ns-cloud-a3.googledomains.com	Zones on DNS server	216.239.36.106
NS	21600	ns-cloud-a4.googledomains.com	Zones on DNS server	216.239.38.106

SOA 21600

Mname	ns-cloud-a1.googledomains.com
Rname	cloud-dns-hostmaster.google.com
Serial number	6
Refresh	21600
Retry	3600
Expire	259200
Minimum TTL	300

Domain falabellabanco.com

falabellabanco / com / Subdomains

record type	TTL	value		
A	1799	144.208.127.93		
NS	1800	dns1.registrar-servers.com	Zones on DNS server	156.154.132.200
NS	1800	dns2.registrar-servers.com	Zones on DNS server	156.154.133.200
MX	1800	10 eforward1.registrar-servers.com		162.255.118.51
MX	1800	10 eforward2.registrar-servers.com		162.255.118.52
MX	1800	10 eforward3.registrar-servers.com		162.255.118.51
MX	1800	15 eforward4.registrar-servers.com		162.255.118.61
MX	1800	20 eforward5.registrar-servers.com		162.255.118.62
TXT	1800	v=spf1 include:spf.efwd.registrar-servers.com ~all		

SOA 3601

Mname	dns1.registrar-servers.com
Rname	hostmaster.registrar-servers.com
Serial number	1586356498
Refresh	43200
Retry	3600
Expire	604800
Minimum TTL	3601

CERTIFICADOS

crt.sh ID	Logged At	Not Before	Not After	Matching Identities	Issuer Name
2679565519	2020-04-08	2020-04-08	2020-07-07	falabellacmr.chilemobile.net	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
2679351888	2020-04-08	2020-04-08	2020-07-07	bci.chilemobile.net	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
2679351879	2020-04-08	2020-04-08	2020-07-07	falabella.chilemobile.net	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3

Subject DN	CN=falabellabanco.com
Issuer DN	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
Serial	273993884659722249600798153450282162059368
Validity	2020-04-08 13:43:44 **to** 2020-07-07 13:43:44 (90 days, 0:00:00)
Names	falabellabanco.com

IP DE ORIGEN DONDE SE ALOJA SITIO

Domain falabella.chilemobile.net is located on IP address << 212.237.63.113 >>

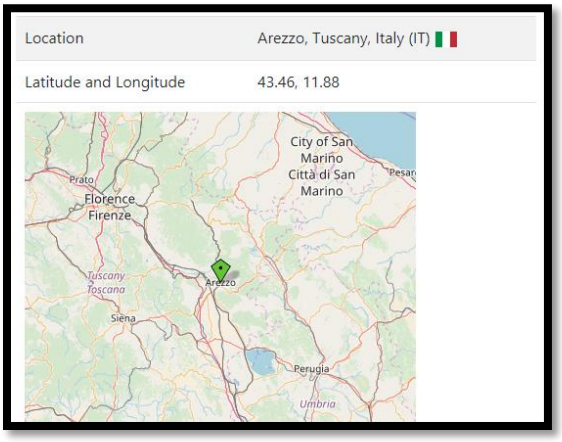
Block start	212.237.63.0
End of block	212.237.63.255
Block size	256 Domains in block
Block name	ARUBA-NET
AS number	31034
Parent block	212.237.0.0 - 212.237.63.255
Organization	Aruba S.p.A. - Cloud Services Farm2

Domain falabellabanco.com is located on IP address << 144.208.127.93 >>

Block start	144.208.127.0
End of block	144.208.127.255
Block size	256 Domains in block
Block name	SH-335
AS number	395092
Parent block	144.208.0.0 - 144.208.127.255
Organization	Shock Hosting LLC

LOCALIZACIÓN

Arezzo, Tuscany, Italia



Piscataway, New Jersey, Estados Unidos

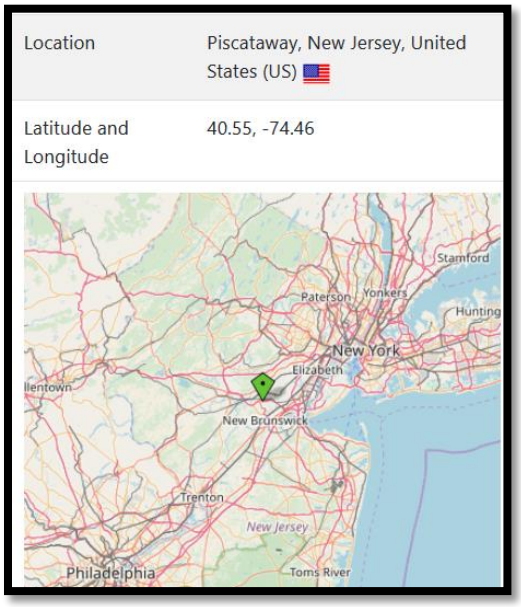
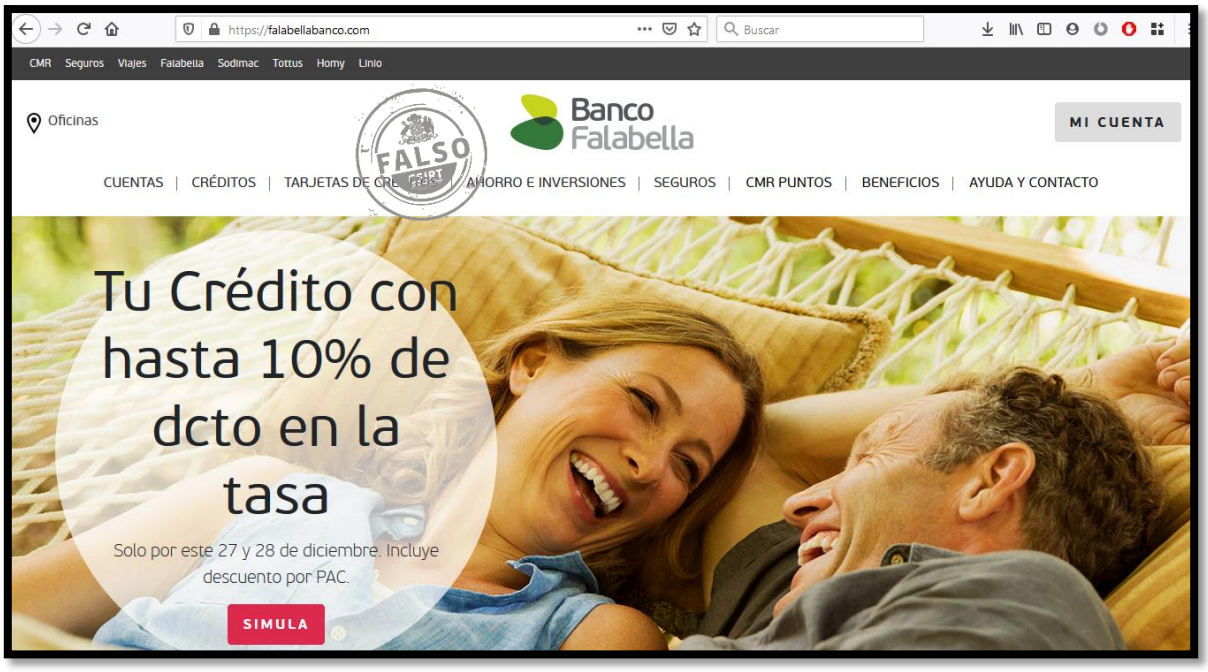


IMAGEN DEL SITIO


https://falabellabanco.com
Buscar
CMR Seguros Viajes Falabella Sodimac Tottus Homy Linio
Oficinas
FALSO
Banco Falabella
MI CUENTA
CUENTAS | CRÉDITOS | TARJETAS DE CRÉ | AHORRO E INVERSIONES | SEGUROS | CMR PUNTOS | BENEFICIOS | AYUDA Y CONTACTO
Tu Crédito con hasta 10% de dcto en la tasa
Solo por este 27 y 28 de diciembre. Incluye descuento por PAC.
SIMULA

WHOIS

```
Domain Name: chilemobile.net
Registry Domain ID: 2512272656_DOMAIN_NET-VRSN
Registrar WHOIS Server: whois.google.com
Registrar URL: https://domains.google.com
Updated Date: 2020-04-08T04:41:09Z
Creation Date: 2020-04-08T04:41:08Z
Registrar Registration Expiration Date: 2021-04-08T04:41:08Z
Registrar: Google LLC
Registrar IANA ID: 895
Registrar Abuse Contact Email: registrar-abuse@google.com
Registrar Abuse Contact Phone: +1.8772376466
Domain Status: clientTransferProhibited https://www.icann.org/epp#clientTransferProhibited
Registry Registrant ID:
Registrant Name: Contact Privacy Inc. Customer 1246876951
Registrant Organization: Contact Privacy Inc. Customer 1246876951
Registrant Street: 96 Mowat Ave
Registrant City: Toronto
Registrant State/Province: ON
Registrant Postal Code: M4K 3K1
Registrant Country: CA
Registrant Phone: +1.4165385487
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: fo93b9kqn1lb@contactprivacy.email
Registry Admin ID:
Admin Name: Contact Privacy Inc. Customer 1246876951
Admin Organization: Contact Privacy Inc. Customer 1246876951
Admin Street: 96 Mowat Ave
Admin City: Toronto
Admin State/Province: ON
Admin Postal Code: M4K 3K1
Admin Country: CA
Admin Phone: +1.4165385487
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: fo93b9kqn1lb@contactprivacy.email
Registry Tech ID:
Tech Name: Contact Privacy Inc. Customer 1246876951
Tech Organization: Contact Privacy Inc. Customer 1246876951
Tech Street: 96 Mowat Ave
Tech City: Toronto
Tech State/Province: ON
Tech Postal Code: M4K 3K1
Tech Country: CA
Tech Phone: +1.4165385487
Tech Phone Ext:
Tech Fax:
Tech Fax Ext:
Tech Email: fo93b9kqn1lb@contactprivacy.email
Name Server: NS-CLOUD-A1.GOOGLEDOMAINS.COM
Name Server: NS-CLOUD-A2.GOOGLEDOMAINS.COM
Name Server: NS-CLOUD-A3.GOOGLEDOMAINS.COM
Name Server: NS-CLOUD-A4.GOOGLEDOMAINS.COM
```

```
Domain name: falabellabanco.com
Registry Domain ID: 2512276275_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.namecheap.com
Registrar URL: http://www.namecheap.com
Updated Date: 0001-01-01T00:00:00.00Z
Creation Date: 2020-04-08T05:33:39.00Z
Registrar Registration Expiration Date: 2021-04-08T05:33:39.00Z
Registrar: NAMECHEAP INC
Registrar IANA ID: 1068
Registrar Abuse Contact Email: abuse@namecheap.com
Registrar Abuse Contact Phone: +1.6613102107
Reseller: NAMECHEAP INC
Domain Status: ok https://icann.org/epp#ok
Domain Status: addPeriod https://icann.org/epp#addPeriod
Registry Registrant ID:
Registrant Name: WhoisGuard Protected
Registrant Organization: WhoisGuard, Inc.
Registrant Street: P.O. Box 0823-03411
Registrant City: Panama
Registrant State/Province: Panama
Registrant Postal Code:
Registrant Country: PA
Registrant Phone: +507.8365503
Registrant Phone Ext:
Registrant Fax: +51.17057182
Registrant Fax Ext:
Registrant Email: 91981f5a7cb34d9f8eb37026097a8d66.protect@whoisguard.com
Registry Admin ID:
Admin Name: WhoisGuard Protected
Admin Organization: WhoisGuard, Inc.
Admin Street: P.O. Box 0823-03411
Admin City: Panama
Admin State/Province: Panama
Admin Postal Code:
Admin Country: PA
Admin Phone: +507.8365503
Admin Phone Ext:
Admin Fax: +51.17057182
Admin Fax Ext:
Admin Email: 91981f5a7cb34d9f8eb37026097a8d66.protect@whoisguard.com
Registry Tech ID:
Tech Name: WhoisGuard Protected
Tech Organization: WhoisGuard, Inc.
Tech Street: P.O. Box 0823-03411
Tech City: Panama
Tech State/Province: Panama
Registry Tech ID:
Tech Name: WhoisGuard Protected
Tech Organization: WhoisGuard, Inc.
Tech Street: P.O. Box 0823-03411
Tech City: Panama
Tech State/Province: Panama
Tech Postal Code:
Tech Country: PA
Tech Phone: +507.8365503
Tech Phone Ext:
Tech Fax: +51.17057182
Tech Fax Ext:
Tech Email: 91981f5a7cb34d9f8eb37026097a8d66.protect@whoisguard.com
Name Server: dns1.registrar-servers.com
Name Server: dns2.registrar-servers.com
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2020-04-08T03:23:09.60Z <<<
```

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: 2020.04.09 16:18:46 -04'00'