Alerta de seguridad cibernética	8FFR20-00323-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	08 de abril de 2020
Última revisión	08 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 tres portales fraudulentos asociados a una IP 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
banco[.]falabellaacesso[.]com
movil[.]falabellacmrcl[.]com
banco[.]falabellacmrcl[.]com

IP
212[.]237[.]63[.]113
212[.]237[.]63[.]113

DOMINIOS DONDE SE ALOJA URL

Domain movil.falabellacmrcl.com

movil / falabellacmrcl / com / Subdomains

record type	TTL	value
A	3600	212.237.63.113

Domain banco.falabellacmrcl.com

banco / falabellacmrcl / com / Subdomains

record type	TTL	value
A	3600	212.237.63.113

Domain falabellacmrcl.com

falabellacmrcl / com / 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	4
		Refresh	21600
		Retry	3600
		Expire	259200
		Minimum TTL	300

Domain falabellaacesso.com

falabellaacesso / com / Subdomains

record type	TTL	value		
NS	21600	ns-cloud-c1.googledomains.com	Zones on DNS server	216.239.32.108
NS	21600	ns-cloud-c2.googledomains.com	Zones on DNS server	216.239.34.108
NS	21600	ns-cloud-c3.googledomains.com	Zones on DNS server	216.239.36.108
NS	21600	ns-cloud-c4.googledomains.com	Zones on DNS server	216.239.38.108

SOA	21600		
		Mname	ns-cloud-c1.googledomains.com
		Rname	cloud-dns-hostmaster.google.com
		Serial number	3
		Refresh	21600
		Retry	3600
		Expire	259200
		Minimum TTL	300

CERTIFICADOS

crt.sh ID	Logged At	Not Before	Not After	Matching Identities	Issuer Name
2671826148	2020-04-06	2020-04-06	2020-07-05	movil.falabellacmrcl.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
2672432396	2020-04-06	2020-04-06	2020-07-05	movil.falabellacmrcl.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3

crt.sh ID	Logged At	Not Before	Not After	Matching Identities	Issuer Name
2671825793	2020-04-06	2020-04-06	2020-07-05	banco.falabellacmrcl.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
2671826936	2020-04-06	2020-04-06	2020-07-05	banco.falabellacmrcl.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3

crt.sh ID	Logged At	Not Before	Not After	Matching Identities	Issuer Name
2665233237	2020-04-04	2020-04-04	2020-07-03	banco.falabellaacesso.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
2665267723	2020-04-04	2020-04-04	2020-07-03	banco.falabellaacesso.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3

IP DE ORIGEN DONDE SE ALOJA SITIO

Domain banco.falabellacmrcl.com 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 movil.falabellacmrcl.com 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 banco.falabellaacesso.com 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

LOCALIZACIÓN

Arezzo, Tuscany, Italia

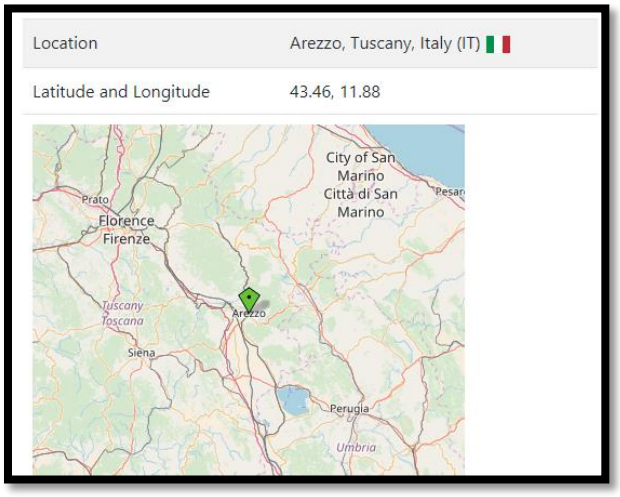
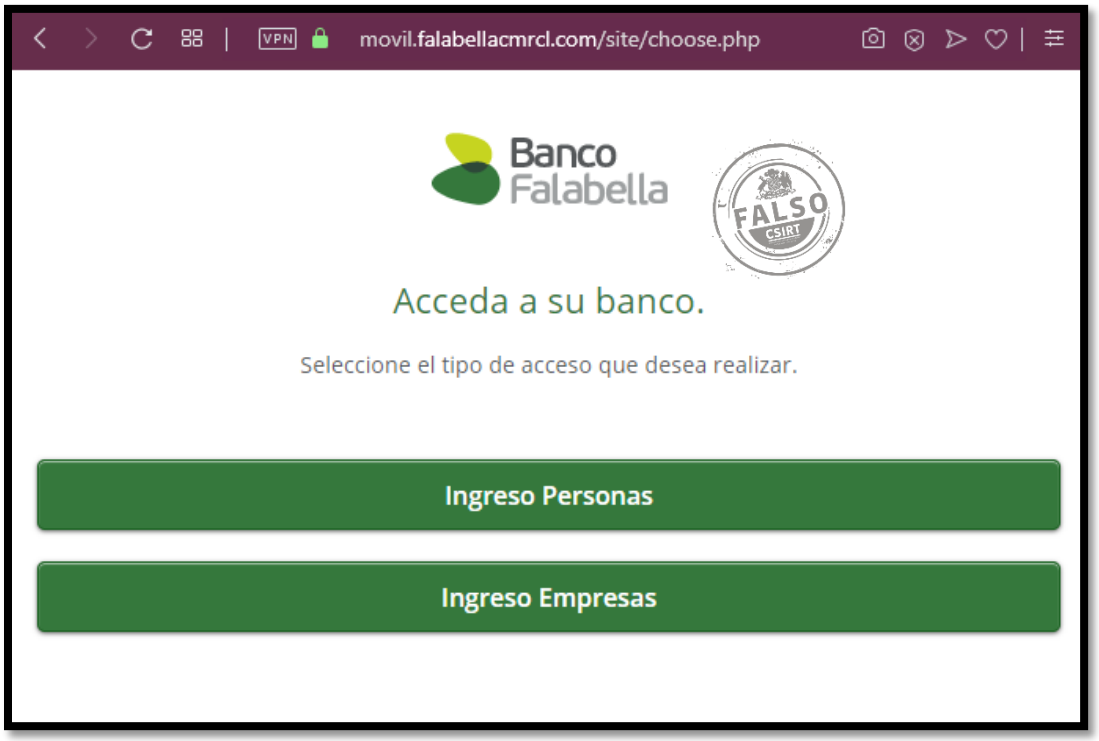
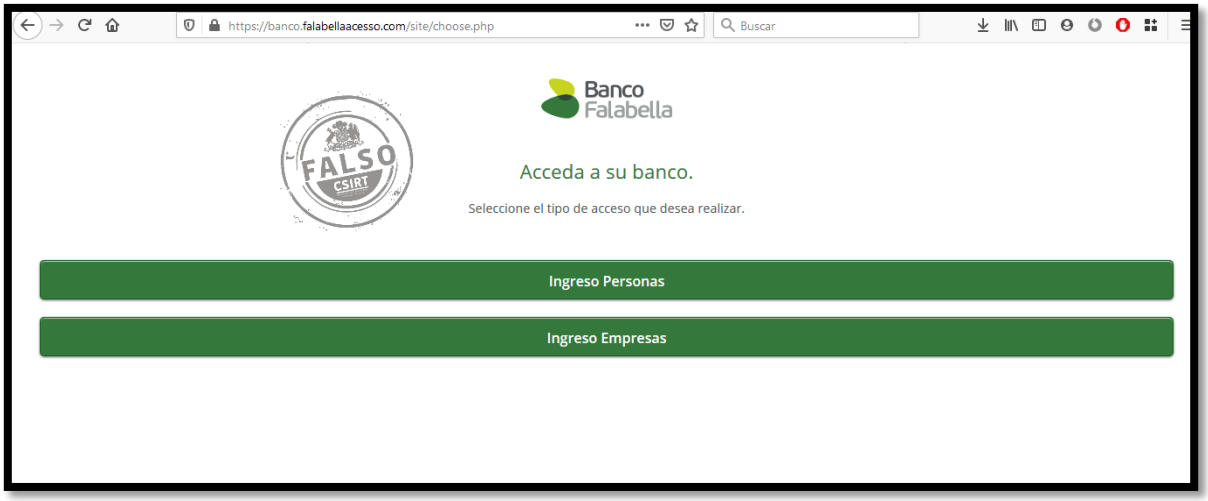


IMAGEN DEL SITIO




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


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

WHOIS

```
Domain Name: falabellaacesso.com
Registry Domain ID: 2510844147_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.google.com
Registrar URL: https://domains.google.com
Updated Date: 2020-04-04T05:21:13Z
Creation Date: 2020-04-04T05:21:11Z
Registrar Registration Expiration Date: 2021-04-04T05:21:11Z
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#clientTransfer
Prohibited
Registry Registrant ID:
Registrant Name: Contact Privacy Inc. Customer 1246844562
Registrant Organization: Contact Privacy Inc. Customer 1246844562
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: skzvqecx11g0@contactprivacy.email
Registry Admin ID:
Admin Name: Contact Privacy Inc. Customer 1246844562
Admin Organization: Contact Privacy Inc. Customer 1246844562
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: skzvqecx11g0@contactprivacy.email
Registry Tech ID:
Tech Name: Contact Privacy Inc. Customer 1246844562
Tech Organization: Contact Privacy Inc. Customer 1246844562
Tech Street: 96 Mowat Ave
Tech City: Toronto
Tech State/Province: ON
```

```
Registry Tech ID:
Tech Name: Contact Privacy Inc. Customer 1246844562
Tech Organization: Contact Privacy Inc. Customer 1246844562
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: skzvqecx1lg0@contactprivacy.email
Name Server: NS-CLOUD-C1.GOOGLEDOMAINS.COM
Name Server: NS-CLOUD-C2.GOOGLEDOMAINS.COM
Name Server: NS-CLOUD-C3.GOOGLEDOMAINS.COM
Name Server: NS-CLOUD-C4.GOOGLEDOMAINS.COM
DNSSEC: signedDelegation
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2020-04-07T18:46:15Z <<<
```

```
Domain Name: FALABELLACMRCL.COM
Registry Domain ID: 2511523577_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.google.com
Registrar URL: http://domains.google.com
Updated Date: 2020-04-06T02:16:29Z
Creation Date: 2020-04-06T02:16:28Z
Registry Expiry Date: 2021-04-06T02:16:28Z
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://icann.org/epp#clientTransferProhibited
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
DNSSEC: signedDelegation
DNSSEC DS Data: 60892 8 2 48A61BA38A62BAEB7B3E8DA9CD8524995 0A462821087464 5B079EEB990538C2D
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: 2020.04.08 12:45:04 -04'00'