Alerta de seguridad informática	8FFR20-00256-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	11 de Marzo de 2020
Última revisión	11 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 una IP que suplantan el sitio web oficial del **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 Compromisos

URL´s

cad-fala[.]ne
cad-fala[.]net/d/

Domain cad-fala.net

cad-fala / net / Subdomains

record type	TTL	value		
A	3600	91.210.107.54		
NS	3600	ns2.argondns.net	Zones on DNS server	101.99.80.106
NS	3600	ns1.argondns.net	Zones on DNS server	101.99.78.111
MX	3600	0 cad-fala.net		
TXT	3600	v=spf1 +a +mx +ip4:91.210.107.22 ~all		
SOA	3600	Mname	ns1.argondns.net	
		Rname	notification.kbreaders.com	
		Serial number	2020030809	
		Refresh	3600	
		Retry	1800	
		Expire	1209600	
		Minimum TTL	86400	

Ilustración 1 Dominio donde se Aloja Url del Banco Falabella y DNS que utiliza

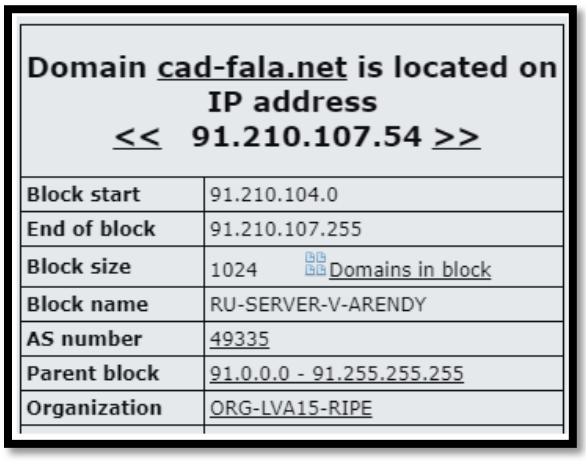
Certificados

Certificates

crt.sh ID	Logged At	Not Before	Not After	Matching Identities	Issuer Name
2553910456	2020-03-08	2020-03-08	2020-06-06	d.cad-fala.net www.d.cad-fala.net	C=US, ST=TX, L=Houston, O="cPanel, Inc.", CN="cPanel, Inc. Certification Authority"
2553910448	2020-03-08	2020-03-08	2020-06-06	d.cad-fala.net www.d.cad-fala.net	C=US, ST=TX, L=Houston, O="cPanel, Inc.", CN="cPanel, Inc. Certification Authority"
2553583888	2020-03-08	2020-03-08	2020-06-06	cad-fala.net cpanel.cad-fala.net cpcalendars.cad-fala.net cpcontacts.cad-fala.net mail.cad-fala.net webdisk.cad-fala.net webmail.cad-fala.net www.cad-fala.net	C=US, ST=TX, L=Houston, O="cPanel, Inc.", CN="cPanel, Inc. Certification Authority"
2553583757	2020-03-08	2020-03-08	2020-06-06	cad-fala.net cpanel.cad-fala.net cpcalendars.cad-fala.net cpcontacts.cad-fala.net mail.cad-fala.net webdisk.cad-fala.net webmail.cad-fala.net www.cad-fala.net	C=US, ST=TX, L=Houston, O="cPanel, Inc.", CN="cPanel, Inc. Certification Authority"

Ilustración 2 Certificado Utilizado en Url del sitio Falso del Banco Falabella

IP
91[.]210[.]107[.]54



Domain cad-fala.net is located on IP address << 91.210.107.54 >>	
Block start	91.210.104.0
End of block	91.210.107.255
Block size	1024 Domains in block
Block name	RU-SERVER-V-ARENDY
AS number	49335
Parent block	91.0.0.0 - 91.255.255.255
Organization	ORG-LVA15-RIPE

Ilustración 3 Ip de Origen donde se aloja Sitio Falso del Banco Falabella

Localización
Rusia

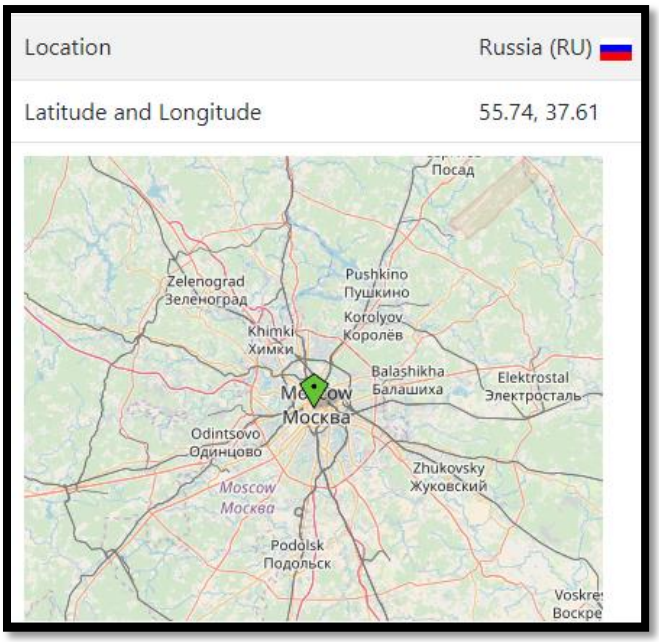
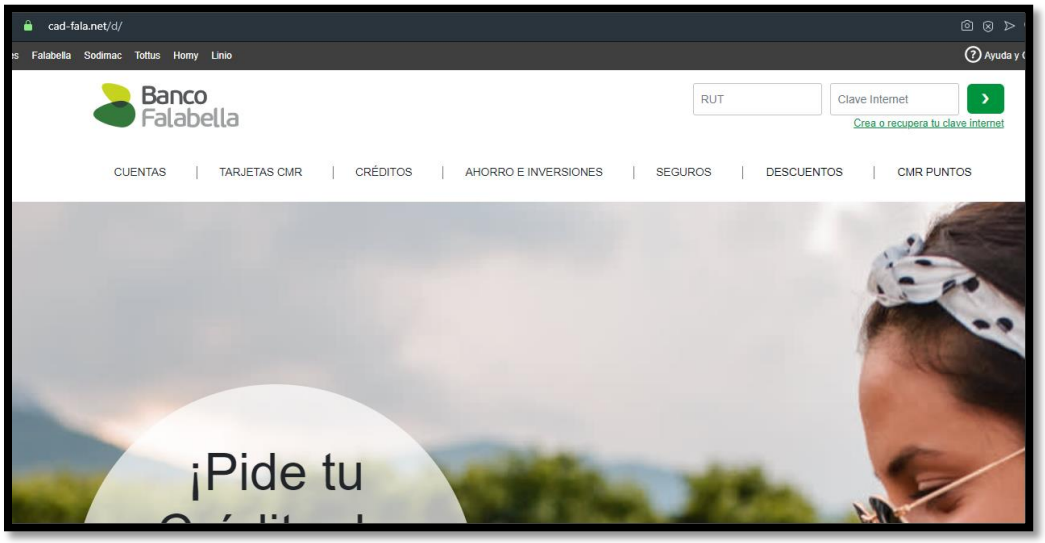


Imagen del sitio



Whois

```
Domain Name: CAD-FALA.NET
Registry Domain ID: 2501144816_DOMAIN_NET-VRSN
Registrar WHOIS Server: whois.ilovewww.com
Registrar URL: http://www.ilovewww.com
Updated Date: 2020-03-08T17:03:52Z
Creation Date: 2020-03-08T17:03:50Z
Registrar Registration Expiration Date: 2021-03-08T17:03:50Z
Registrar: Shinjiru MSC Sdn Bhd
Registrar IANA ID: 1741
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProh
ibited
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: ns1.argondns.net
Name Server: ns2.argondns.net
DNSSEC: Unsigned
Registrar Abuse Contact Email: abuse@ilovewww.com
Registrar Abuse Contact Phone: +603 2031 8850
```

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: 2020.03.11 22:34:16 -03'00'