Alerta de seguridad informática	8FFR20-00425-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	20 de Mayo de 2020
Última revisión	20 de Mayo 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 de Chile**, 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
bancochile.cl[.]bouph[.]com
bchile[.]mcblack1[.]com

IP
142[.]11[.]253[.]177
213[.]108[.]242[.]100

Dominios donde se aloja url

Domain mcblack1.com

mcblack1 / com / Subdomains

record type	TTL	value		
A	14400	142.11.253.177		
NS	86400	dalns160.hostwindsdns.com	Zones on DNS server	142.11.249.228
NS	86400	dalns159.hostwindsdns.com	Zones on DNS server	142.11.249.186
MX	14400	0 mcblack1.com		
TXT	14400	v=spf1 +a +mx +ip4:142.11.249.186 +ip4:142.11.253.177 ~all		

SOA	86400		
		Mname	dalns159.hostwindsdns.com
		Rname	dallasshared.hostwinds.com
		Serial number	2020051903
		Refresh	3600
		Retry	1800
		Expire	1209600
		Minimum TTL	86400

Domain bouph.com

bouph / com / Subdomains

record type	TTL	value		
A	14400	213.108.242.100		
NS	86400	ns3.dadetejarat.com	Zones on DNS server	213.108.242.100
NS	86400	ns4.dadetejarat.com	Zones on DNS server	213.108.242.100
NS	86400	ns5.dadetejarat.com	Zones on DNS server	213.108.242.100
NS	86400	ns6.dadetejarat.com	Zones on DNS server	213.108.242.100
MX	14400	0 bouph.com		
TXT	14400	v=spf1 ip4:213.108.242.100 +a +mx ~all		

SOA	86400		
		Mname	ns3.dadetejarat.com
		Rname	dadetejarat.gmail.com
		Serial number	2020051913
		Refresh	3600
		Retry	1800
		Expire	1209600
		Minimum TTL	86400

Certificados

Certificates	crt.sh ID	Logged At ⇧	Not Before	Not After	Matching Identities	Issuer Name
	2828944955	2020-05-19	2020-05-19	2020-08-17	bchile.mcblack1.com www.bchile.mcblack1.com	C=US, ST=TX, L=Houston, O="cPanel, Inc.", CN="cPanel, Inc. Certification Authority"
	2828944401	2020-05-19	2020-05-19	2020-08-17	bchile.mcblack1.com www.bchile.mcblack1.com	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
	2830116071	2020-05-19	2020-05-19	2020-08-17	www3.bancochile.cl.bouph.com www.www3.bancochile.cl.bouph.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	2830092608	2020-05-19	2020-05-19	2020-08-17	bancochile.cl.bouph.com www.bancochile.cl.bouph.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3

Ip de origen donde se aloja sitio

Domain bchile.mcblack1.com is located on IP address << 142.11.253.177 >>

Block start	142.11.192.0
End of block	142.11.255.255
Block size	16384 Domains in block
Block name	HOSTWINDS-18-1
AS number	54290
Parent block	142.0.0.0 - 142.255.255.255
Organization	HostwindsLLC.

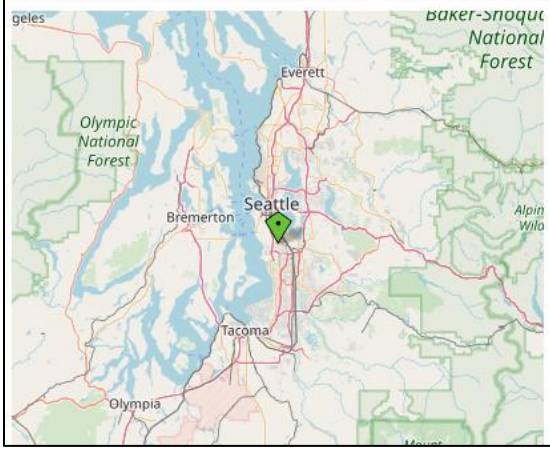
Domain bancochile.cl.bouph.com is located on IP address << 213.108.242.100 >>

Block start	213.108.242.0
End of block	213.108.242.255
Block size	256 Domains in block
Block name	Gameserverprovider
AS number	200296
Parent block	213.108.240.0 - 213.108.243.255
Organization	

Localización

Seattle, Washington, Estados Unidos

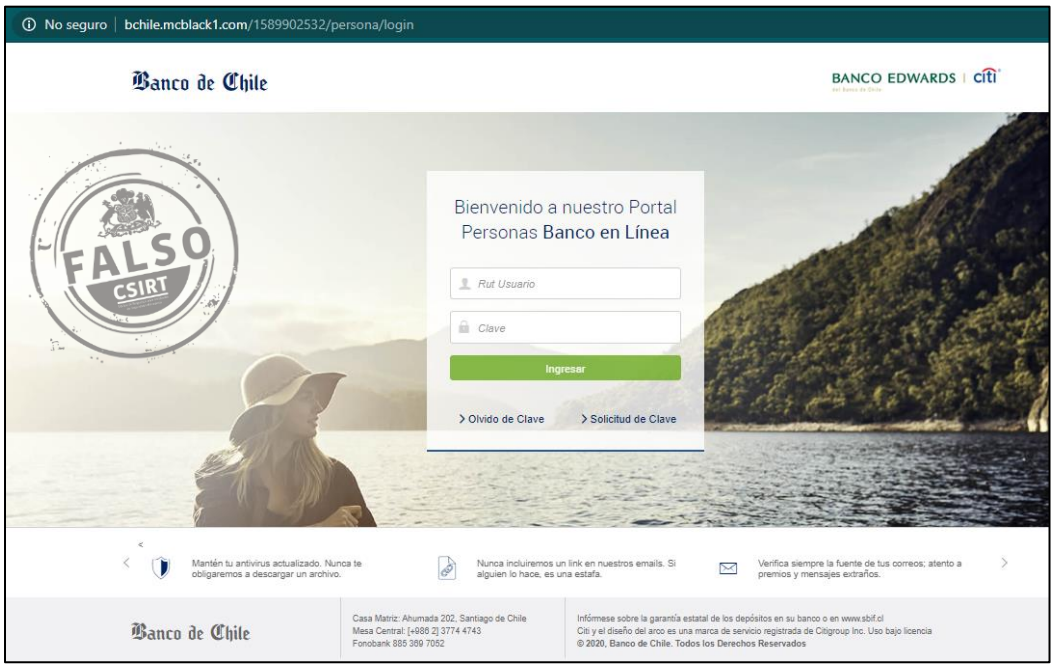
Location	Seattle, Washington, United States (US)
Latitude and Longitude	47.49, -122.3

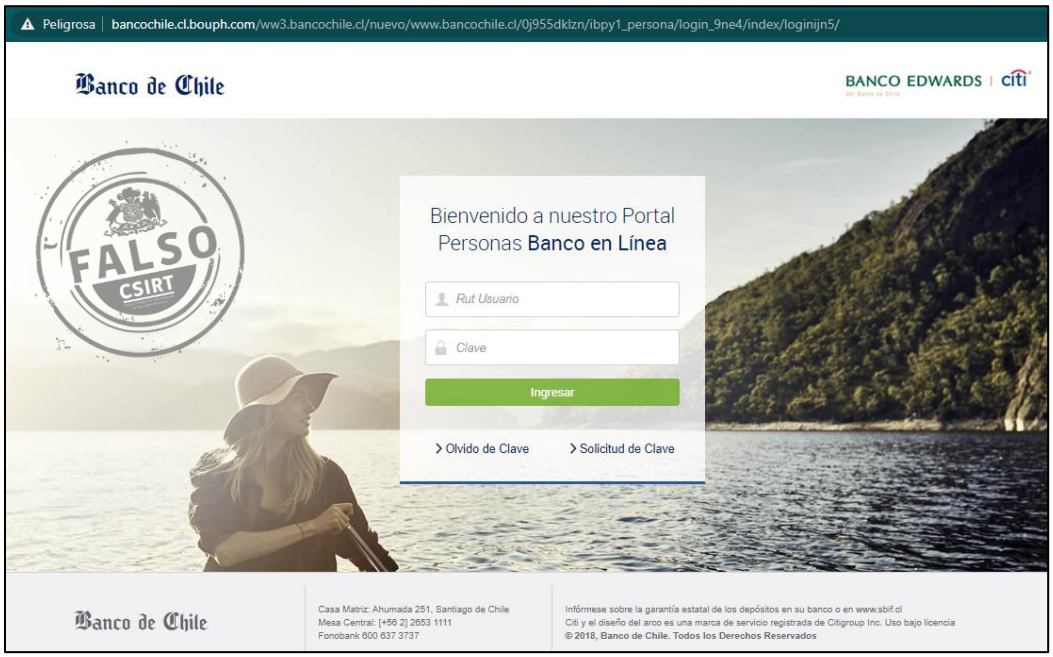


Emiratos Árabes Unidos

Location	United Arab Emirates (AE)
Latitude and Longitude	24, 54

Imagen del sitio





Whois

```
Domain Name: mcblack1.com
Registry Domain ID: 2441663905_DOMAIN_COM-VRSN
Registrar WHOIS Server: WHOIS.ENOM.COM
Registrar URL: WWW.ENOM.COM
Updated Date: 2019-10-08T19:26:27.00Z
Creation Date: 2019-10-08T19:26:00.00Z
Registrar Registration Expiration Date: 2020-10-08T19:26:00.00Z
Registrar: ENOM, INC.
Registrar IANA ID: 48
Domain Status: clientTransferProhibited https://www.icann.org/epp#clientTransferProhibited
Registrant Name: REDACTED FOR PRIVACY
Registrant Organization: REDACTED FOR PRIVACY
Registrant Street: REDACTED FOR PRIVACY
Registrant Street:
Registrant City: REDACTED FOR PRIVACY
Registrant State/Province: lima
Registrant Postal Code: REDACTED FOR PRIVACY
Registrant Country: PE
Registrant Phone: REDACTED FOR PRIVACY
Registrant Phone Ext:
Registrant Fax: REDACTED FOR PRIVACY
Registrant Email: https://tieredaccess.com/contact/459d5270-2c28-4780-95e4-9ba5af7ba1ba
Admin Name: REDACTED FOR PRIVACY
Admin Organization: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
Admin Street:
Admin City: REDACTED FOR PRIVACY
Admin State/Province: REDACTED FOR PRIVACY
Admin Postal Code: REDACTED FOR PRIVACY
Admin Country: REDACTED FOR PRIVACY
Admin Phone: REDACTED FOR PRIVACY
Admin Phone Ext:
Admin Fax: REDACTED FOR PRIVACY
Admin Email: REDACTED FOR PRIVACY
Tech Name: REDACTED FOR PRIVACY
Tech Organization: REDACTED FOR PRIVACY
Tech Street: REDACTED FOR PRIVACY
Tech Street:
Tech City: REDACTED FOR PRIVACY
Tech State/Province: REDACTED FOR PRIVACY
Tech Postal Code: REDACTED FOR PRIVACY
Tech Country: REDACTED FOR PRIVACY
Tech Phone: REDACTED FOR PRIVACY
Tech Phone Ext:
Tech Fax: REDACTED FOR PRIVACY
Tech Email: REDACTED FOR PRIVACY
Name Server: DALNS159.HOSTWINDSDNS.COM
Name Server: DALNS160.HOSTWINDSDNS.COM
DNSSEC: unsigned
```

```
Domain Name: BOUPH.COM
Registry Domain ID: 2523904490_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.1api.net
Registrar URL: http://www.1api.net
Updated Date: 2020-05-09T11:56:11Z
Creation Date: 2020-05-09T11:56:11Z
Registrar Registration Expiration Date: 2021-05-09T11:56:11Z
Registrar: 1API GmbH
Registrar IANA ID: 1387
Registrar Abuse Contact Email: abuse@1api.net
Registrar Abuse Contact Phone: +49.68416984×200
Domain Status: clientTransferProhibited - http://www.icann.org/epp#clientTransferProhibited
Registry Registrant ID:
Registrant Name: REDACTED FOR PRIVACY
Registrant Organization: REDACTED FOR PRIVACY
Registrant Street: REDACTED FOR PRIVACY
Registrant City: REDACTED FOR PRIVACY
Registrant State/Province: azarbayjan sharghi
Registrant Postal Code: REDACTED FOR PRIVACY
Registrant Country: AZ
Registrant Phone: REDACTED FOR PRIVACY
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: contact via https://www.1api.net/send-message/bouph.com/registrant
Registry Admin ID:
Admin Name: REDACTED FOR PRIVACY
Admin Organization: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
Admin City: REDACTED FOR PRIVACY
Admin State/Province: REDACTED FOR PRIVACY
Admin Postal Code: REDACTED FOR PRIVACY
Admin Country: REDACTED FOR PRIVACY
Admin Phone: REDACTED FOR PRIVACY
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: contact via https://www.1api.net/send-message/bouph.com/admin
Registry Tech ID:
Tech Name: REDACTED FOR PRIVACY
Tech Organization: REDACTED FOR PRIVACY
Tech Street: REDACTED FOR PRIVACY
Tech City: REDACTED FOR PRIVACY
Tech State/Province: REDACTED FOR PRIVACY
Tech Postal Code: REDACTED FOR PRIVACY
Tech Country: REDACTED FOR PRIVACY
Tech Phone: REDACTED FOR PRIVACY
Tech Phone Ext:
Tech Fax:
Tech Fax Ext:
Tech Email: contact via https://www.1api.net/send-message/bouph.com/tech
Name Server: ns3.dadetejarat.com 213.108.242.100
Name Server: ns4.dadetejarat.com 213.108.242.100
DNSSEC: unsigned
```

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.