Alerta de seguridad cibernética	8FFR20-00322-01
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 dos portales fraudulentos asociados a una IP que suplantan el sitio web oficial de Banco BCI, 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
clientesbci[.]com
clientesbci[.]com/inicio[.]jsf

IP
167[.]114[.]126[.]57

DOMINIOS DONDE SE ALOJA URL

Domain clientesbci.com

clientesbci / com / Subdomains

record type	TTL	value		
A	14400	167.114.126.57		
NS	86400	ns2.hostinguard.pe	Zones on DNS server	167.114.126.57
NS	86400	ns1.hostinguard.pe	Zones on DNS server	167.114.126.57
MX	14400	0 clientesbci.com		
TXT	14400	v=spf1 +a +mx +ip4:167.114.126.57 ~all		
SOA	86400	Mname	ns1.hostinguard.pe	
		Rname	admin.desarrolloweb.com	
		Serial number	2020040702	
		Refresh	3600	
		Retry	1800	
		Expire	1209600	
		Minimum TTL	86400	

CERTIFICADOS

crt.sh ID	Logged At	Not Before	Not After	Matching Identities	Issuer Name
2677625309	2020-04-07	2020-04-07	2020-07-06	clientesbci.com cpanel.clientesbci.com cpcalendars.clientesbci.com cpcontacts.clientesbci.com mail.clientesbci.com webdisk.clientesbci.com webmail.clientesbci.com www.clientesbci.com	C=US, ST=TX, L=Houston, O="cPanel, Inc.", CN="cPanel, Inc. Certification Authority"
2677625333	2020-04-07	2020-04-07	2020-07-06	clientesbci.com cpanel.clientesbci.com cpcalendars.clientesbci.com cpcontacts.clientesbci.com mail.clientesbci.com webdisk.clientesbci.com webmail.clientesbci.com www.clientesbci.com	C=US, ST=TX, L=Houston, O="cPanel, Inc.", CN="cPanel, Inc. Certification Authority"

IP DE ORIGEN DONDE SE ALOJA SITIO

Domain clientesbci.com is located on IP address << 167.114.126.57 >>	
Block start	167.114.0.0
End of block	167.114.255.255
Block size	65536 Domains in block
Block name	ASHTON
AS number	16276
Parent block	167.0.0.0 - 167.255.255.255
Organization	OVH Hosting, Inc.

LOCALIZACIÓN

Montreal, Quebec, Canadá

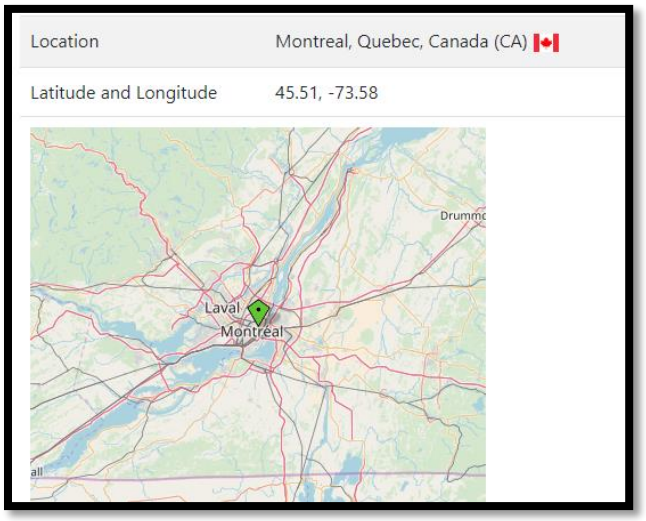
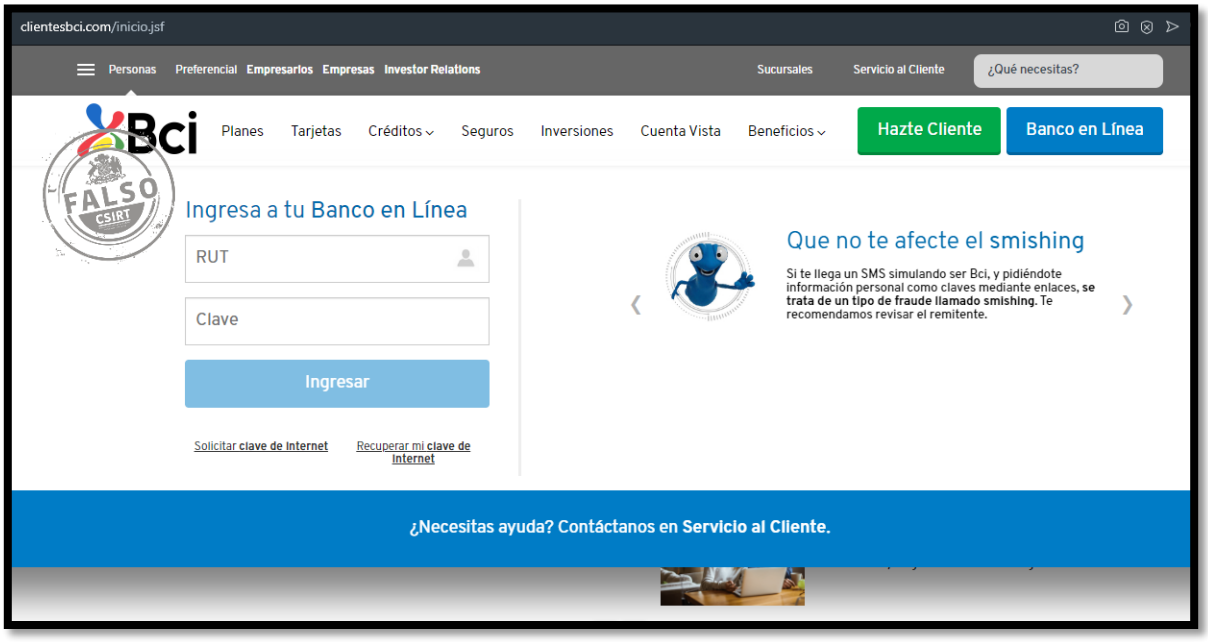


IMAGEN DEL SITIO



WHOIS

```
Domain Name: CLIENTESBCI.COM
Registry Domain ID: 2511979487_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.name.com
Registrar URL: http://www.name.com
Updated Date: 2020-04-07T14:08:03Z
Creation Date: 2020-04-07T14:08:02Z
Registrar Registration Expiration Date: 2021-04-07T14:08:02Z
Registrar: Name.com, Inc.
Registrar IANA ID: 625
Reseller:
Domain Status: addPeriod https://www.icann.org/epp#addPeriod
Domain Status: clientTransferProhibited https://www.icann.org/epp#clientTransferProhibited
Registry Registrant ID: Not Available From Registry
Registrant Name: Whois Agent
Registrant Organization: Domain Protection Services, Inc.
Registrant Street: PO Box 1769
Registrant City: Denver
Registrant State/Province: CO
Registrant Postal Code: 80201
Registrant Country: US
Registrant Phone: +1.7208009072
Registrant Fax: +1.7209758725
Registrant Email: https://www.name.com/contact-domain-whois/clientesbci.com
Registry Admin ID: Not Available From Registry
Admin Name: Whois Agent
Admin Organization: Domain Protection Services, Inc.
Admin Street: PO Box 1769
Admin City: Denver
Admin State/Province: CO
Admin Postal Code: 80201
Admin Country: US
Admin Phone: +1.7208009072
Admin Fax: +1.7209758725
Admin Email: https://www.name.com/contact-domain-whois/clientesbci.com
Registry Tech ID: Not Available From Registry
Tech Name: Whois Agent
Tech Organization: Domain Protection Services, Inc.
Tech Street: PO Box 1769
Tech City: Denver
Tech State/Province: CO
Tech Postal Code: 80201
Tech Country: US
Tech Phone: +1.7208009072
Tech Fax: +1.7209758725
Tech Email: https://www.name.com/contact-domain-whois/clientesbci.com
Name Server: ns1.hostinguard.pe
Name Server: ns2.hostinguard.pe
DNSSEC: unSigned
Registrar Abuse Contact Email: abuse@name.com
Registrar Abuse Contact Phone: +1.7203101849
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2020-04-07T19:21:49Z <<<

For more information on Whois status codes, please visit https://icann.org/epp
```

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 11:54:37 -04'00'