Alerta de seguridad informática	8FFR20-00281-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 de Marzo de 2020
Última revisión	24 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 dos IPs 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

mdk-clientes[.]xyz/4QeE9o95XQaYVAhpd/cl/bci/aplicaciones/contenido/personas

bcicl[.]com

bcicl[.]com/inicio[.]jsf

IP

103[.]116[.]16[.]4

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

DOMINIOS DONDE SE ALOJA URL

Domain mdk-clientes.xyz

mdk-clientes / xyz / Subdomains

record type	TTL	value		
A	14400	103.116.16.4		
NS	86400	blue22.yourserversdns.com	Zones on DNS server	162.219.251.2
NS	86400	blue21.yourserversdns.com	Zones on DNS server	174.127.88.195
MX	14400	0 mdk-clientes.xyz		
SOA	86400	Mname: blue21.yourserversdns.com Rname: vasocareproducts.gmail.com Serial number: 2020032003 Refresh: 86400 Retry: 7200 Expire: 3600000 Minimum TTL: 86400		

Domain bcicl.com

bcicl / 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 bcicl.com		
TXT	14400	v=spf1 +a +mx +ip4:167.114.126.57 ~all		
SOA	86400	Mname: ns1.hostinguard.pe Rname: admin.hostinguard.pe Serial number: 2020032004 Refresh: 3600 Retry: 1800 Expire: 1209600 Minimum TTL: 86400		

CERTIFICADOS

Certificates

crt.sh ID	Logged At	Not Before	Not After	Matching Identities	Issuer Name
2604559166	2020-03-20	2020-03-20	2020-06-18	autodiscover.mdk-clientes.xyz cpanel.mdk-clientes.xyz mail.mdk-clientes.xyz mdk-clientes.xyz webdisk.mdk-clientes.xyz webmail.mdk-clientes.xyz www.mdk-clientes.xyz	C=US, ST=TX, L=Houston, O="cPanel, Inc.", CN="cPanel, Inc. Certification Authority"
2604559059	2020-03-20	2020-03-20	2020-06-18	autodiscover.mdk-clientes.xyz cpanel.mdk-clientes.xyz mail.mdk-clientes.xyz mdk-clientes.xyz webdisk.mdk-clientes.xyz webmail.mdk-clientes.xyz www.mdk-clientes.xyz	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
2604340988	2020-03-20	2020-03-20	2020-06-18	bcicl.com mail.bcicl.com www.bcicl.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
2604342030	2020-03-20	2020-03-20	2020-06-18	bcicl.com mail.bcicl.com www.bcicl.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
2604334964	2020-03-20	2020-03-20	2020-06-18	bcicl.com cpanel.bcicl.com cpcalendars.bcicl.com cpcontacts.bcicl.com mail.bcicl.com webdisk.bcicl.com webmail.bcicl.com www.bcicl.com	C=US, ST=TX, L=Houston, O="cPanel, Inc.", CN="cPanel, Inc. Certification Authority"
2604335005	2020-03-20	2020-03-20	2020-06-18	bcicl.com cpanel.bcicl.com cpcalendars.bcicl.com cpcontacts.bcicl.com mail.bcicl.com webdisk.bcicl.com webmail.bcicl.com www.bcicl.com	C=US, ST=TX, L=Houston, O="cPanel, Inc.", CN="cPanel, Inc. Certification Authority"

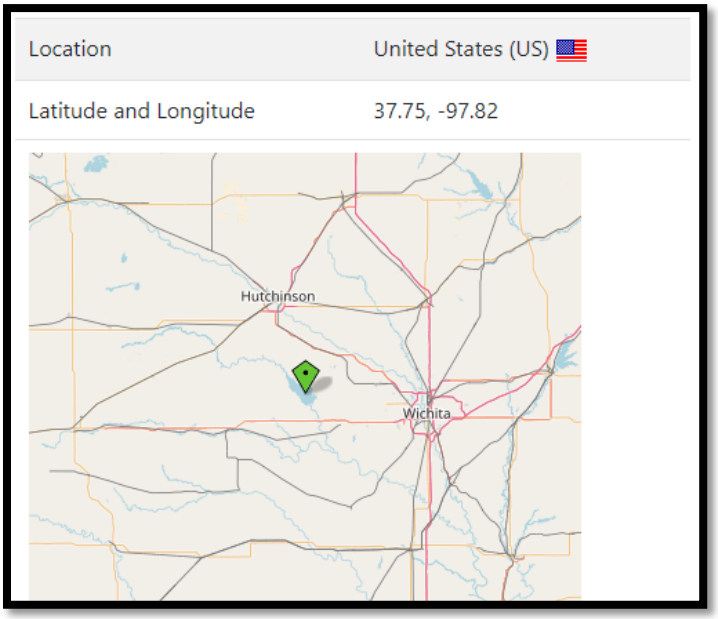
IP DE ORIGEN DONDE SE ALOJA SITIO

Domain mdk-clientes.xyz is located on IP address << 103.116.16.4 >>	
Block start	103.116.16.0
End of block	103.116.17.255
Block size	512 Domains in block
Block name	IHNET-AP
AS number	137870
Parent block	103.0.0.0 - 103.255.255.255
Organization	IHNetworks, LLC

Domain bcicl.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

Hutchinson, Estados Unidos
Montreal, Quebec, Canada



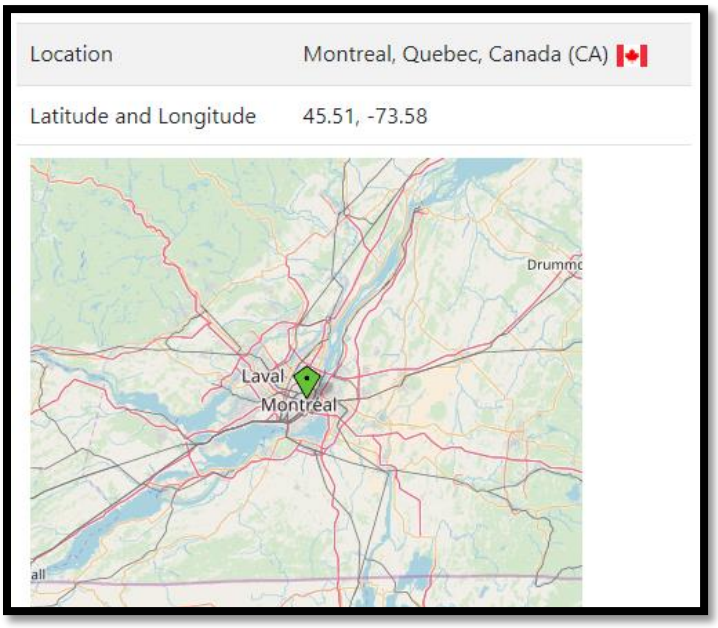
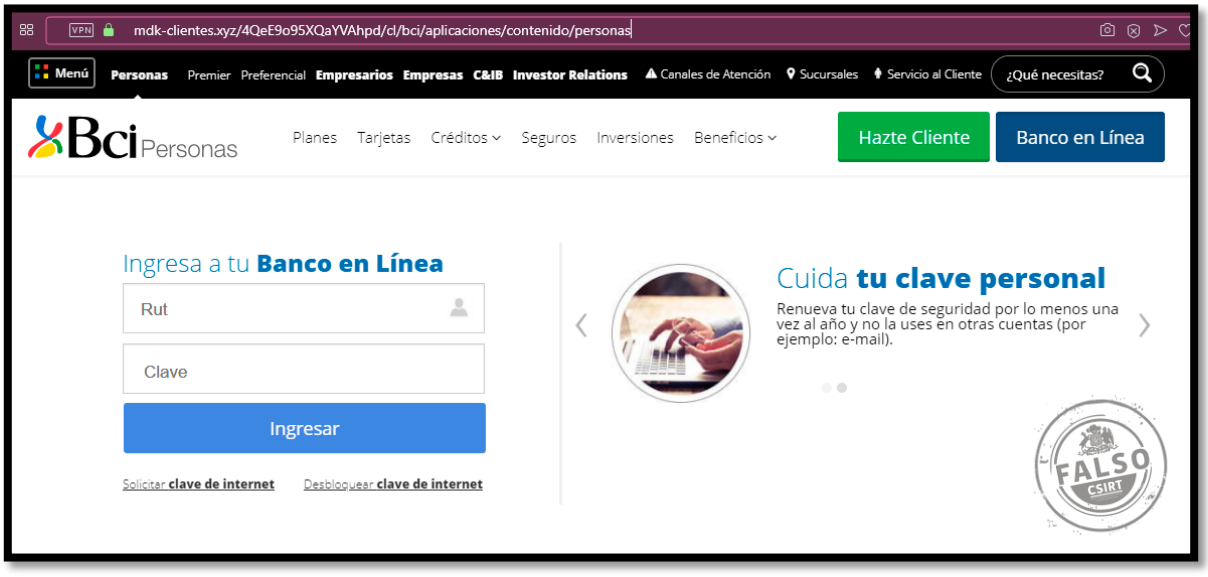
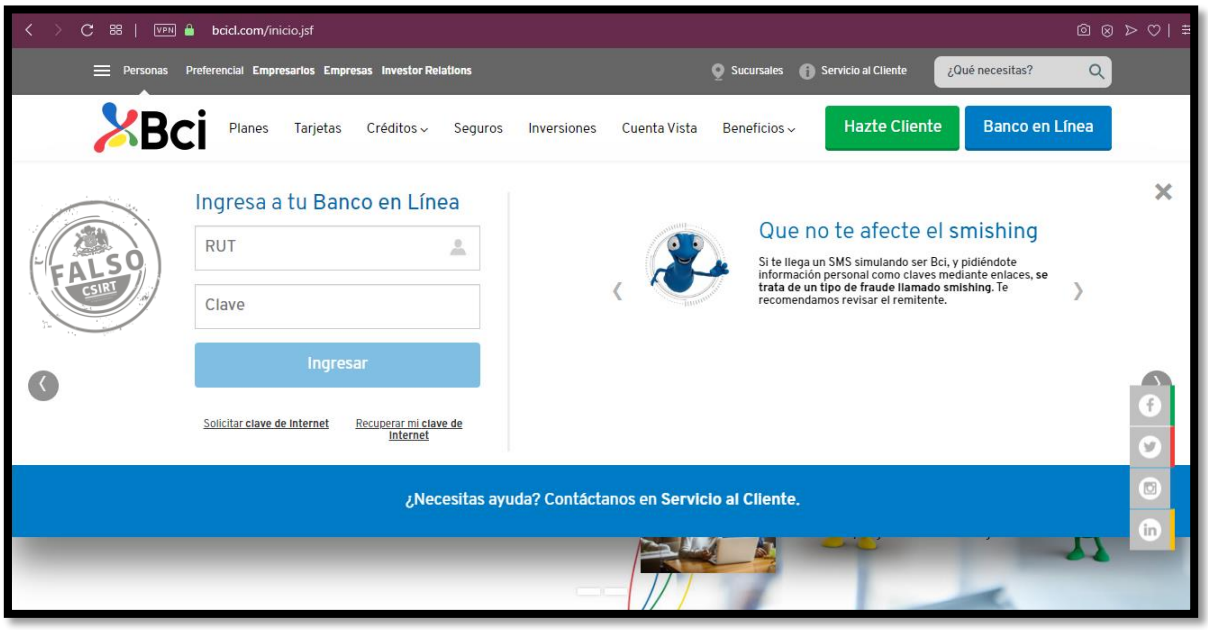


IMAGEN DEL SITIO





WHOIS

```
Domain Name: BCICL.COM
Registry Domain ID: 2505341043_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.nominalia.com
Registrar URL: http://www.nominalia.com
Updated Date: 2020-03-20T00:00:00Z
Creation Date: 2020-03-20T00:00:00Z
Registrar Registration Expiration Date: 2021-03-20T00:00:00Z
Registrar: NOMINALIA INTERNET S.L.
Registrar IANA ID: 76
Registrar Abuse Contact Email: abuse@nominalia.com
Registrar Abuse Contact Phone: +39.05520021555
Reseller:
Domain Status: ok https://icann.org/epp#ok
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: Coronel portillo
Registrant Postal Code: REDACTED FOR PRIVACY
Registrant Country: PE
Registrant Phone: REDACTED.FORPRIVACY
Registrant Phone Ext:
Registrant Fax: REDACTED.FORPRIVACY
Registrant Fax Ext:
Registrant Email: https://domaincontact.nominalia.com/contact-domain
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: Coronel portillo
Admin Postal Code: REDACTED FOR PRIVACY
Admin Country: PE
Admin Phone: REDACTED.FORPRIVACY
Admin Phone Ext:
Admin Fax: REDACTED.FORPRIVACY
Admin Fax Ext:
Admin Email: https://domaincontact.nominalia.com/contact-domain
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: Barcelona
Tech Postal Code: REDACTED FOR PRIVACY
Tech Country: ES
Tech Phone: REDACTED.FORPRIVACY
Tech Phone Ext:
Tech Fax: REDACTED.FORPRIVACY
Tech Fax Ext:
Tech Email: https://domaincontact.nominalia.com/contact-domain
Name Server: NS1.HOSTINGUARD.PE
Name Server: NS2.HOSTINGUARD.PE
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of whois database: 2020-03-23T16:30:08Z <<<
```

```
root@ITQ-ivps3:~# whois mdk-clientes.xyz
Domain Name: MDK-CLIENTES.XYZ
Registry Domain ID: D179433624-CNIC
Registrar WHOIS Server: whois.instra.net
Registrar URL:
Updated Date: 2020-03-20T13:22:53.0Z
Creation Date: 2020-03-20T05:09:50.0Z
Registry Expiry Date: 2021-03-20T23:59:59.0Z
Registrar: Instra Corporation Pty Ltd
Registrar IANA ID: 1376
Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
Domain Status: addPeriod https://icann.org/epp#addPeriod
Registrant Organization: Registrant of mdk-clientes.xyz
Registrant State/Province: Auckland District
Registrant Country: NZ
Registrant Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech co
ntact of the queried domain name.
Admin Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact
 of the queried domain name.
Tech Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact
of the queried domain name.
Name Server: BLUE21.YOURSERVERSDNS.COM
Name Server: BLUE22.YOURSERVERSDNS.COM
DNSSEC: unsigned
Billing Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech conta
ct of the queried domain name.
Registrar Abuse Contact Email: compliance@instra.com
Registrar Abuse Contact Phone:
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of WHOIS database: 2020-03-23T15:38:17.0Z <<<
```

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: 2020.03.24 14:07:16 -03'00'