Alerta de seguridad informática	8FFR-00110-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	12 de Noviembre de 2019
Última revisión	12 de Noviembre de 2019

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 un portal fraudulento asociado a una IP que suplanta 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 Compromisos

URL´s

https://bnchilee[.]com/persona/login/

https://www[.]technostoremm[.]com/wp-content/uploads/elementor/css/servicio/servicios[.]transferencia[.]bancoedwards[.]cl/r0m7h3igf5/wb36w_persona/login_f28l/index/loginz6ov/

Domain bnchilee.com

bnchilee / com / Subdomains

record type	TTL	value		
A	14400	66.165.231.59		
NS	86400	ns-us06.webhostcluster.com	Zones on DNS server	66.165.241.60
NS	86400	ns-us05.webhostcluster.com	Zones on DNS server	66.165.231.60
MX	14400	0 bnchilee.com		
TXT	14400	v=spf1 +a +mx +ip4:66.165.231.58 include:relay.mailchannels.net ~all		
SOA	86400	Mname: ns-us05.webhostcluster.com Rname: srvmonitor.mechanicweb.com Serial number: 2019111102 Refresh: 3600 Retry: 1800 Expire: 1209600 Minimum TTL: 86400		

Domain technostoremm.com

technostoremm / com / Subdomains

record type	TTL	value		
A	14400	85.187.131.105		
NS	86400	ns3.supercp.com	Zones on DNS server	162.159.24.28
NS	86400	ns4.supercp.com	Zones on DNS server	162.159.25.237
NS	86400	ns2.supercp.com	Zones on DNS server	162.159.25.30
NS	86400	ns1.supercp.com	Zones on DNS server	162.159.24.43
MX	14400	0 technostoremm.com		
TXT	14400	v=spf1 ip4:85.187.128.19 +a +mx +ip4:85.187.131.105 ~all		
SOA	86400	Mname: ns1.supercp.com Rname: laragoisen2019.yandex.com Serial number: 2019093001 Refresh: 3600 Retry: 1800 Expire: 1209600 Minimum TTL: 86400		

Ilustración 1 Dominio donde se Aloja Url del Banco Chile, Falso y DNS que utiliza

Certificado

Criteria	Identity = 'bnchilee.com'

Certificates

crt.sh ID	Logged At	Not Before	Not After	Issuer Name
2099001369	2019-11-11	2019-11-11	2020-02-09	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
2099001320	2019-11-11	2019-11-11	2020-02-09	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
2098269646	2019-11-11	2019-11-11	2020-02-09	C=US, ST=TX, L=Houston, O="cPanel, Inc.", CN="cPanel, Inc. Certification Authority"
2098268409	2019-11-11	2019-11-11	2020-02-09	C=US, ST=TX, L=Houston, O="cPanel, Inc.", CN="cPanel, Inc. Certification Authority"

Criteria	Identity = 'technostoremm.com'

Certificates

crt.sh ID	Logged At	Not Before	Not After	Issuer Name
1896586074	2019-09-13	2019-09-13	2019-12-12	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1879527259	2019-09-13	2019-09-13	2019-12-12	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1897682611	2019-09-11	2019-09-11	2019-12-10	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1871137372	2019-09-11	2019-09-11	2019-12-10	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3

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

IP´s

66[.]165[.]231[.]59

85[.]187[.]131[.]105

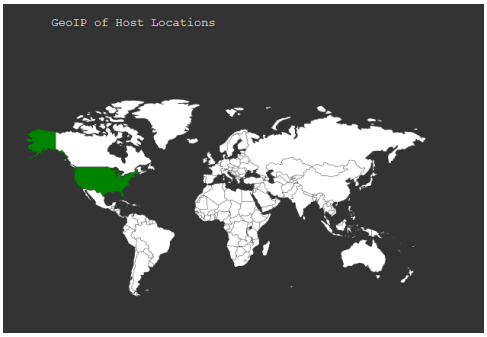
Domain bnchilee.com is located on IP address << 66.165.231.59 >>	
Block start	66.165.224.0
End of block	66.165.255.255
Block size	8192 Domains in block
Block name	CYBERWORLD-INT
AS number	29802
Parent block	66.0.0.0 - 66.255.255.255
Organization	Cyber World Internet Services, Inc.
City	Liberty Lake
Region/State	Washington
Country	US , United States
Reg. date	2003-09-15
Host name	la02.webhostcluster.com
Domains	1 bnchilee.com

Domain technostoremm.com is located on IP address << 85.187.131.105 >>	
Block start	85.187.128.0
End of block	85.187.159.255
Block size	8192 Domains in block
Block name	US-A2HOS-20041126
AS number	55293
Parent block	85.0.0.0 - 85.255.255.255
Organization	ORG-AHI1-RIPE
City	Ann Arbor
Region/State	Michigan
Country	US , United States
Reg. date	2004-11-26
Host name	85.187.131.105.static.supercp.com
Domains	1 technostoremm.com

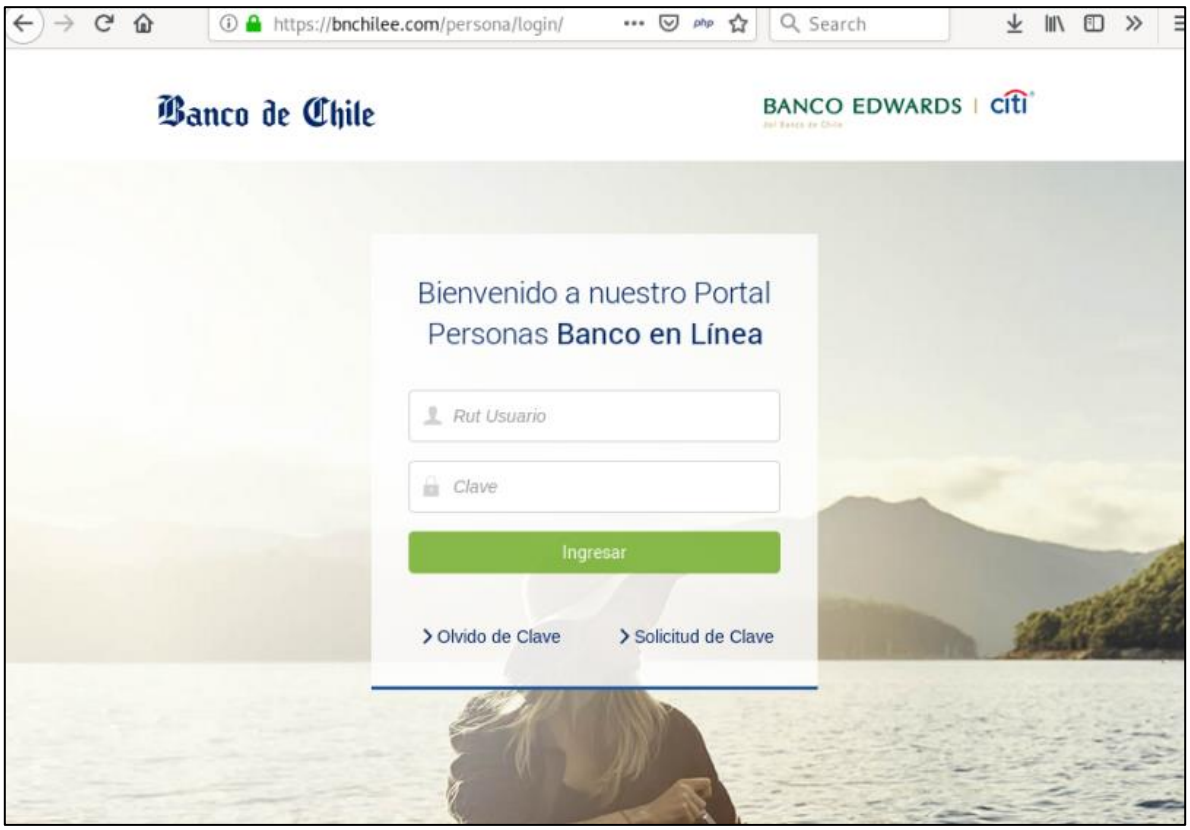
Ilustración 3 Ip de Origen donde se aloja Sitio Falso del Banco Estado

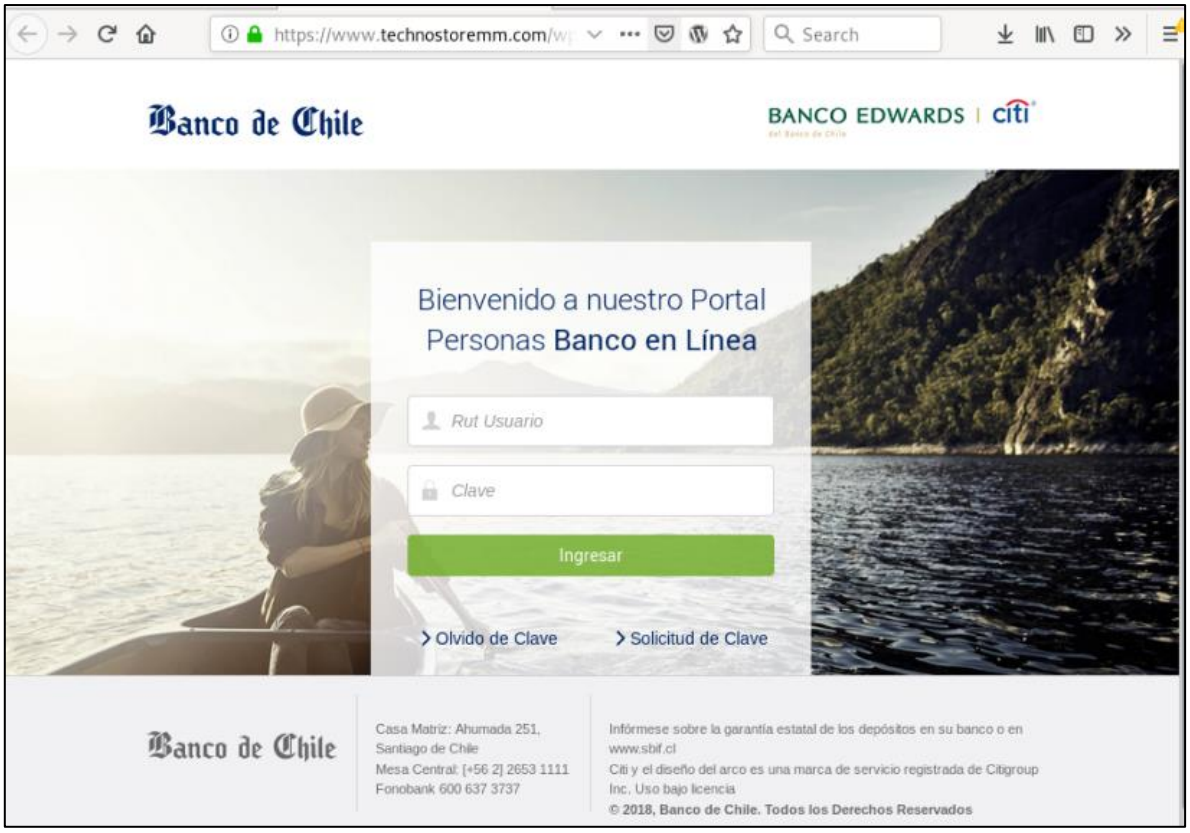
Localización

San Jose, California, Ann Arbor, Michigan, Estados Unidos



Imagen




https://www.technostoremm.com/
Search
Banco de Chile
BANCO EDWARDS | citi
Bienvenido a nuestro Portal
Personas Banco en Línea
Rut Usuario
Clave
Ingresar
Olvido de Clave
Solicitud de Clave
Banco de Chile
Casa Matriz: Ahumada 251,
Santiago de Chile
Mesa Central: [+56 2] 2653 1111
Fonobank 600 637 3737
Infórmese sobre la garantía estatal de los depósitos en su banco o en www.sbif.cl
Citi y el diseño del arco es una marca de servicio registrada de Citigroup Inc. Uso bajo licencia
© 2018, Banco de Chile. Todos los Derechos Reservados

Whois

```
Domain Name: BNCHILEE.COM
Registry Domain ID: 2453760869_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.publicdomainregistry.com
Registrar URL: www.publicdomainregistry.com
Updated Date: 2019-11-11T11:45:16Z
Creation Date: 2019-11-11T11:45:15Z
Registrar Registration Expiration Date: 2020-11-11T11:45:15Z
Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com
Registrar IANA ID: 303
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProh
ibited
Registry Registrant ID: Not Available From Registry
Registrant Name: pier alva
Registrant Organization:
Registrant Street: san isidro 635
Registrant City: santiago
Registrant State/Province: santiago de chile
Registrant Postal Code: 8845670
Registrant Country: CL
Registrant Phone: +56.998099182
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: pieralva385@gmail.com
Registry Admin ID: Not Available From Registry
Admin Name: pier alva
Admin Organization:
Admin Street: san isidro 635
Admin City: santiago
Admin State/Province: santiago de chile
Admin Postal Code: 8845670
Admin Country: CL
Admin Phone: +56.998099182
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: pieralva385@gmail.com
Registry Tech ID: Not Available From Registry
Tech Name: pier alva
Tech Organization:
Tech Street: san isidro 635
Tech City: santiago
Tech State/Province: santiago de chile
Tech Postal Code: 8845670
Tech Country: CL
Tech Phone: +56.998099182
Tech Phone Ext:
Tech Fax:
Tech Fax Ext:
Tech Email: pieralva385@gmail.com
Name Server: ns-us05.webhostcluster.com
Name Server: ns-us06.webhostcluster.com
DNSSEC: Unsigned
Registrar Abuse Contact Email: abuse-contact@publicdomainregistry.com
Registrar Abuse Contact Phone: +1.2013775952
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2019-11-12T14:41:13Z <<<

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

```
Domain Name: technostoremm.com
Registry Domain ID: 2432096544_DOMAIN_COM-VRSN
Registrar WHOIS Server: WHOIS.ENOM.COM
Registrar URL: WWW.ENOM.COM
Updated Date: 2019-09-30T06:14:37.00Z
Creation Date: 2019-09-11T07:28:00.00Z
Registrar Registration Expiration Date: 2020-09-11T07:28:00.00Z
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: Yangon
Registrant Postal Code: REDACTED FOR PRIVACY
Registrant Country: MM
Registrant Phone: REDACTED FOR PRIVACY
Registrant Phone Ext:
Registrant Fax: REDACTED FOR PRIVACY
Registrant Email: https://tieredaccess.com/contact/3c14f861-e1ae-43df-b984-1acc88600b3a
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: NS1.SUPERCP.COM
Name Server: NS2.SUPERCP.COM
Name Server: NS3.SUPERCP.COM
Name Server: NS4.SUPERCP.COM
DNSSEC: unsigned
Registrar Abuse Contact Email: ABUSE@ENOM.COM
Registrar Abuse Contact Phone: +1.4259744689
URL of the ICANN WHOIS Data Problem Reporting System: HTTP://WDPRS.INTERNIC.NET/
>>> Last update of WHOIS database: 2019-11-12T14:53:37.00Z <<<

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: 2019.11.14 15:47:15 -03'00'