Alerta de seguridad informática	8FFR20-00228-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	22 de Febrero de 2020
Última revisión	22 de Febrero 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 un portal fraudulento asociado a una IP que suplanta el sitio web oficial del **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

URLs

pocrtalperssocnas-bencochiile-cl[.]bptsd[.]com/ingreso-personas-cl/

Domain bptsd.com

bptsd / com / Subdomains

record type	TTL	value		
A	1200	104.219.248.48		
NS	1800000	dns1.namecheaphosting.com	Zones on DNS server	156.154.132.200
NS	1800000	dns2.namecheaphosting.com	Zones on DNS server	156.154.133.200
MX	1200	10 smx1.web-hosting.com		162.255.118.62, 162.255.118.61
MX	1200	20 smx2.web-hosting.com		162.255.118.61, 162.255.118.62
MX	1200	30 smx3.web-hosting.com		162.255.118.62, 162.255.118.61
TXT	1200	MAltYWlsLmJwdHNkLmNvbS4K		
TXT	1200	v=spf1 +a +mx +ip4:104.219.248.44 include:spf.web-hosting.com ~all		

SOA	1800000		
		Mname	dns1.namecheaphosting.com
		Rname	cpanel.tech.namecheap.com
		Serial number	1582131815
		Refresh	86400
		Retry	7200
		Expire	3600000
		Minimum TTL	86400

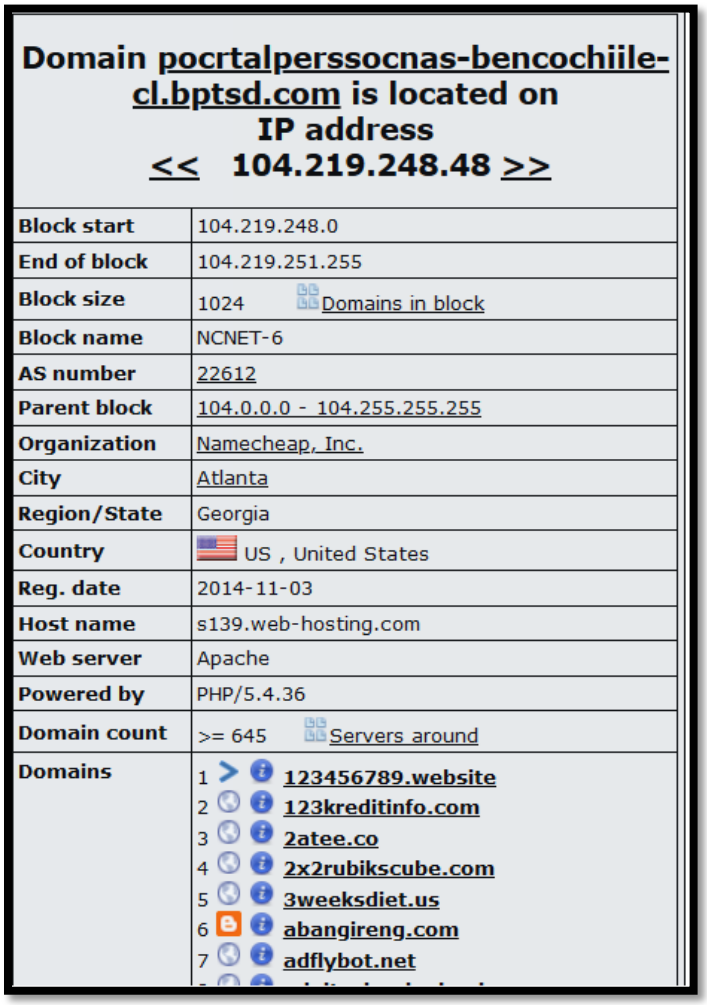
Ilustración 1 Dominio donde se Aloja Url del Banco de Chile, Falso y DNS que utiliza

Certificados

Subject DN	CN=pocrtalperssocnas-bencochiile-cl.bptsd.com
Issuer DN	C=GB, ST=Greater Manchester, L=Salford, O=Sectigo Limited, CN=Sectigo RSA Domain Validation Secure Server CA
Serial	143301494123845248994768474064101767326
Validity	2020-02-19 00:00:00 to 2021-02-18 23:59:59 (365 days, 23:59:59)
Names	pocrtalperssocnas-bencochiile-cl.bptsd.com www.pocrtalperssocnas-bencochiile-cl.bptsd.com

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

IP
104[.]219[.]248[.]48



Domain pocrtalperssocnas-bencochiile-cl.bptsd.com is located on IP address
<< 104.219.248.48 >>

Block start	104.219.248.0
End of block	104.219.251.255
Block size	1024 Domains in block
Block name	NCNET-6
AS number	22612
Parent block	104.0.0.0 - 104.255.255.255
Organization	Namecheap, Inc.
City	Atlanta
Region/State	Georgia
Country	US , United States
Reg. date	2014-11-03
Host name	s139.web-hosting.com
Web server	Apache
Powered by	PHP/5.4.36
Domain count	>= 645 Servers around
Domains	1 123456789.website 2 123kreditinfo.com 3 2atee.co 4 2x2rubikscube.com 5 3weeksdiet.us 6 abangireng.com 7 adflybot.net

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

Localización

Atlanta, Georgia, United States of America

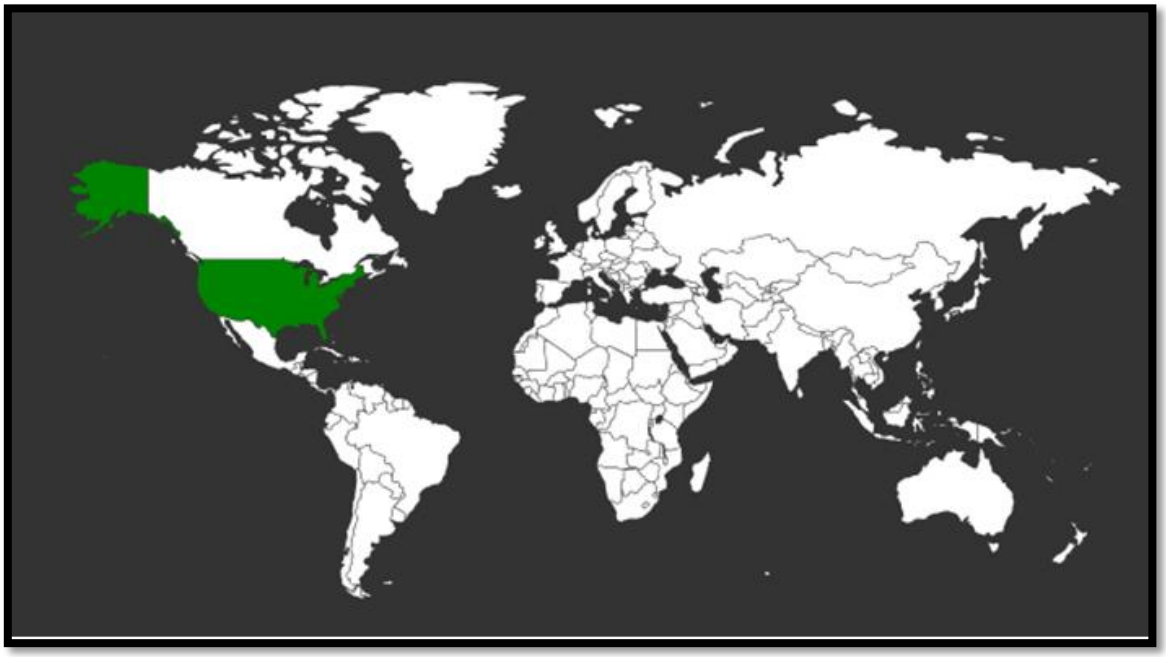
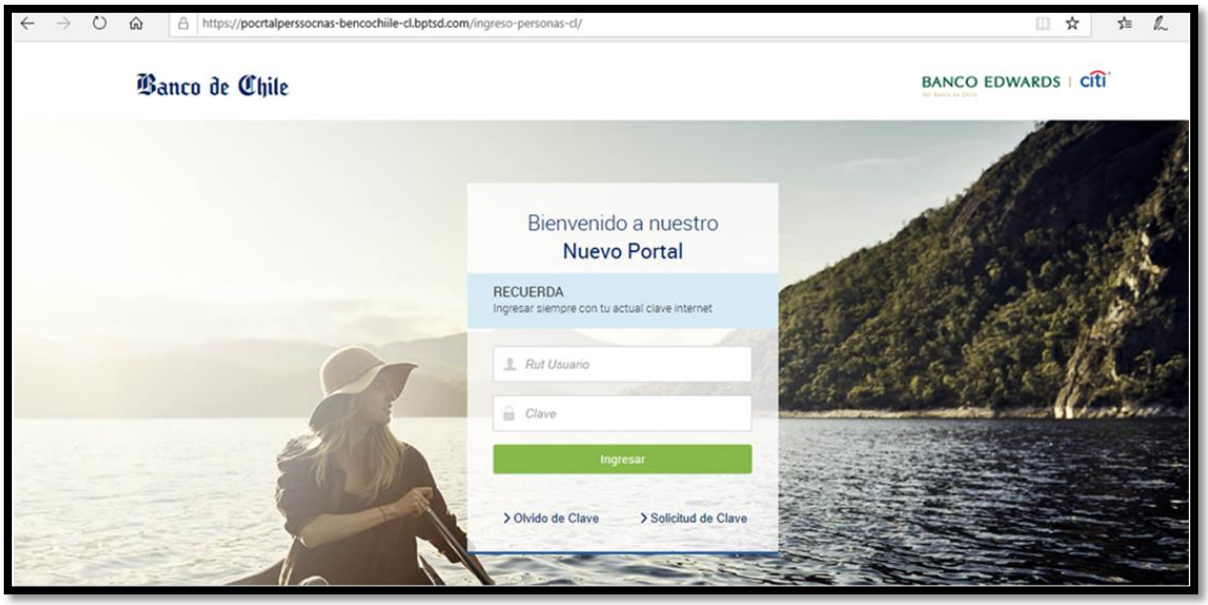


Imagen del sitio



Whois

```
Domain name: bptsd.com
Registry Domain ID: 2494379084_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.namecheap.com
Registrar URL: http://www.namecheap.com
Updated Date: 0001-01-01T00:00:00.00Z
Creation Date: 2020-02-19T16:31:31.00Z
Registrar Registration Expiration Date: 2021-02-19T16:31:31.00Z
Registrar: NAMECHEAP INC
Registrar IANA ID: 1068
Registrar Abuse Contact Email: abuse@namecheap.com
Registrar Abuse Contact Phone: +1.6613102107
Reseller: NAMECHEAP INC
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: addPeriod https://icann.org/epp#addPeriod
Registry Registrant ID:
Registrant Name: WhoisGuard Protected
Registrant Organization: WhoisGuard, Inc.
Registrant Street: P.O. Box 0823-03411
Registrant City: Panama
Registrant State/Province: Panama
Registrant Postal Code:
Registrant Country: PA
Registrant Phone: +507.8365503
Registrant Phone Ext:
Registrant Fax: +51.17057182
Registrant Fax Ext:
Registrant Email: e8074ed6525f43c6a0b3d99ba35e60d5.protect@whoisguard.com
Registry Admin ID:
Admin Name: WhoisGuard Protected
Admin Organization: WhoisGuard, Inc.
Admin Street: P.O. Box 0823-03411
Admin City: Panama
Admin State/Province: Panama
Admin Postal Code:
Admin Country: PA
Admin Phone: +507.8365503
Admin Phone Ext:
Admin Fax: +51.17057182
Admin Fax Ext:
Admin Email: e8074ed6525f43c6a0b3d99ba35e60d5.protect@whoisguard.com
Registry Tech ID:
Tech Name: WhoisGuard Protected
Tech Organization: WhoisGuard, Inc.
Tech Street: P.O. Box 0823-03411
Tech City: Panama
Tech State/Province: Panama
Tech Postal Code:
Tech Country: PA
Tech Phone: +507.8365503
Tech Phone Ext:
Tech Fax: +51.17057182
Tech Fax Ext:
Tech Email: e8074ed6525f43c6a0b3d99ba35e60d5.protect@whoisguard.com
Name Server: dns1.namecheaphosting.com
Name Server: dns2.namecheaphosting.com
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.

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2020.02.22 09:54:00 -03'00'