Alerta de seguridad informática	**8FFR-00095-001**
Clase de alerta	**Fraude**
Tipo de incidente	**Falsificación de Registros o Identidad**
Nivel de riesgo	**Alto**
TLP	**Blanco**
Fecha de lanzamiento original	**18 de Octubre de 2019**
Última revisión	**18 de Octubre 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 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 Compromisos

URL´s

https[://]turismoenperuviajes[.]com/bci[.]cl/empresa/empresas/index[.]php

Domain turismoenperuviajes.com

turismoenperuviajes / com / Subdomains

record type	TTL	value		
A	14400	213.190.6.116		
NS	86400	ns2.hostinger.es	Zones on DNS server	31.220.23.1
NS	86400	ns4.hostinger.es	Zones on DNS server	31.170.164.249
NS	86400	ns3.hostinger.es	Zones on DNS server	173.192.183.247
NS	86400	ns1.hostinger.es	Zones on DNS server	31.170.163.241
MX	14400	10 mx1.hostinger.es		145.14.159.241, 185.224.136.6
TXT	14400	v=spf1 include:spf.mx.hostinger.com include:relay.mailchannels.net ~all		
SOA	86400	Mname	ns1.hostinger.es	
		Rname	dns.hostinger.com	
		Serial number	2019072822	
		Refresh	28800	
		Retry	7200	
		Expire	604800	
		Minimum TTL	86400	

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

Certificado

Criteria: Identity = 'turismoenperuviajes.com'

Certificates

crt.sh ID	Logged At ⇧	Not Before	Not After	Issuer Name
1989715284	2019-10-11	2019-10-11	2020-01-09	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1985331749	2019-10-11	2019-10-11	2020-01-09	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1772079642	2019-08-12	2019-08-12	2019-11-10	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1762449003	2019-08-12	2019-08-12	2019-11-10	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3

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

IP´s

213[.]190[.]6[.]116

Domain turismoenperuviajes.com is located on IP address << 213.190.6.116 >>	
Block start	213.190.6.0
End of block	213.190.6.255
Block size	256 Domains in block
Block name	HOSTINGER-HOSTING
AS number	47583
Parent block	213.190.4.0 - 213.190.7.255
Organization	ORG-HIL9-RIPE
City	-
Country	
Host name	no record in reverse zone
Domains	1 turismoenperuviajes.com

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

Localización

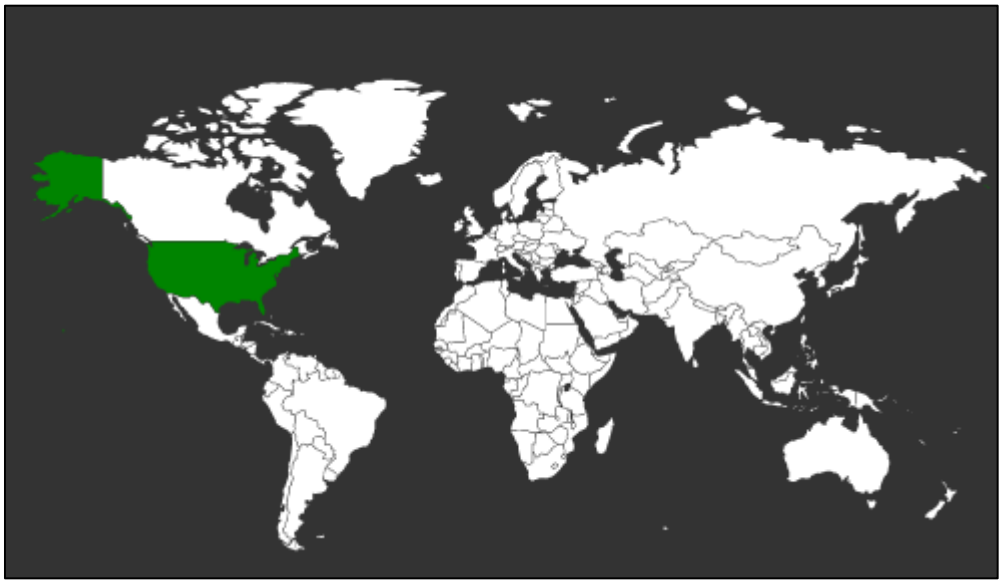
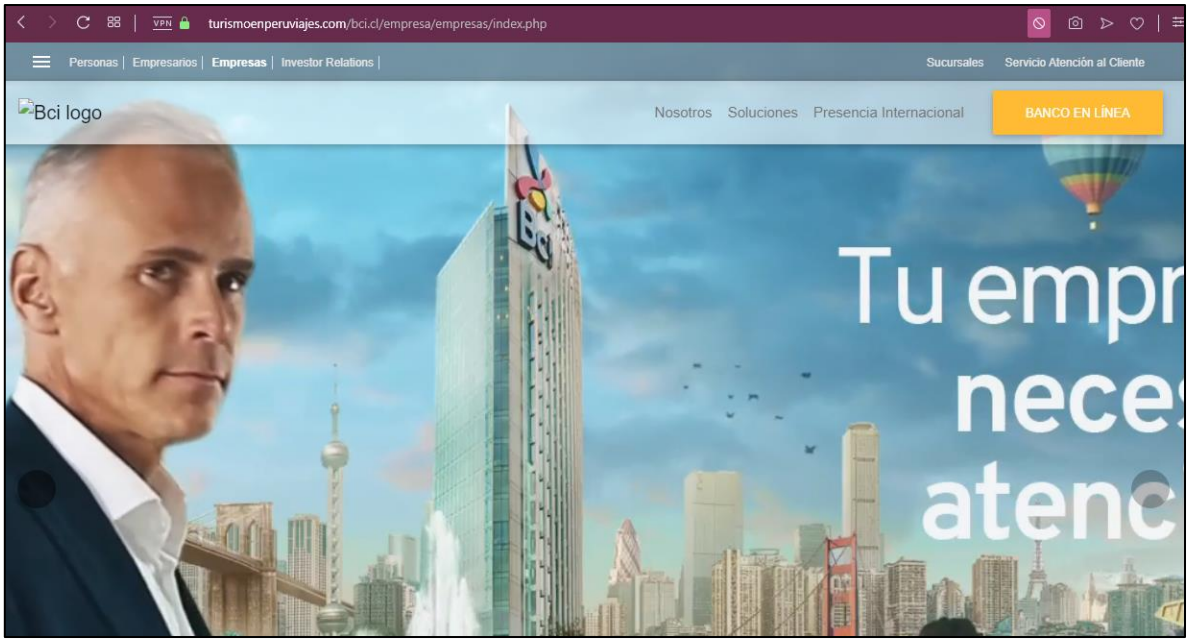


Imagen del sitio



Whois

```
soc@ITQ-ivps3:~$ whois turismoenperuviajes.com
   Domain Name: TURISMOENPERUVIAJES.COM
   Registry Domain ID: 2302310120_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.godaddy.com
   Registrar URL: http://www.godaddy.com
   Updated Date: 2019-08-26T14:33:43Z
   Creation Date: 2018-08-26T04:58:16Z
   Registry Expiry Date: 2020-08-26T04:58:16Z
   Registrar: GoDaddy.com, LLC
   Registrar IANA ID: 146
   Registrar Abuse Contact Email: abuse@godaddy.com
   Registrar Abuse Contact Phone: 480-624-2505
   Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
   Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
   Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
   Name Server: NS1.HOSTINGER.ES
   Name Server: NS2.HOSTINGER.ES
   Name Server: NS3.HOSTINGER.ES
   Name Server: NS4.HOSTINGER.ES
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2019-10-17T13:47:40Z <<<

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

NOTICE: The expiration date displayed in this record is the date the
registrar's sponsorship of the domain name registration in the registry is
currently set to expire. This date does not necessarily reflect the expiration
date of the domain name registrant's agreement with the sponsoring
registrar.  Users may consult the sponsoring registrar's Whois database to
view the registrar's reported date of expiration for this registration.

TERMS OF USE: You are not authorized to access or query our Whois
database through the use of electronic processes that are high-volume and
automated except as reasonably necessary to register domain names or
modify existing registrations; the Data in VeriSign Global Registry
Services' ("VeriSign") Whois database is provided by VeriSign for
information purposes only, and to assist persons in obtaining information
about or related to a domain name registration record. VeriSign does not
guarantee its accuracy. By submitting a Whois query, you agree to abide
by the following terms of use: You agree that you may use this Data only
for lawful purposes and that under no circumstances will you use this Data
to: (1) allow, enable, or otherwise support the transmission of mass
unsolicited, commercial advertising or solicitations via e-mail, telephone,
or facsimile; or (2) enable high volume, automated, electronic processes
that apply to VeriSign (or its computer systems). The compilation,
repackaging, dissemination or other use of this Data is expressly
prohibited without the prior written consent of VeriSign. You agree not to
use electronic processes that are automated and high-volume to access or
query the Whois database except as reasonably necessary to register
domain names or modify existing registrations. VeriSign reserves the right
to restrict your access to the Whois database in its sole discretion to ensure
operational stability.  VeriSign may restrict or terminate your access to the
Whois database for failure to abide by these terms of use. VeriSign
reserves the right to modify these terms at any time.

The Registry database contains ONLY .COM, .NET, .EDU domains and
Registrars.
```

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: 2019.10.18 08:29:57 -03'00'