Alerta de seguridad informática	8FFR20-00219-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	16 de febrero de 2020
Última revisión	16 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 de Banco Itau, 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:

www2[.]scotia[.]chile[.]002l[.]live

Domain 002l.live

002l / live / Subdomains

record type	TTL	value		
A	7207	139.59.63.103		
NS	172800	ns1.dnsowl.com	Zones on DNS server	198.251.84.16, 104.207.141.138, 185.34.216.159
NS	172800	ns2.dnsowl.com	Zones on DNS server	64.32.22.100, 168.235.75.52, 45.32.237.128
NS	172800	ns3.dnsowl.com	Zones on DNS server	209.141.39.150, 45.63.106.63, 45.63.5.234
SOA	172800	Mname	ns1.dnsowl.com	
		Rname	hostmaster.dnsowl.com	
		Serial number	1581691876	
		Refresh	7200	
		Retry	1800	
		Expire	1209600	
		Minimum TTL	600	

Ilustración 1 Dominio donde se aloja URL del Banco Itau falso y DNS que utiliza

Certificados

No existe certificado para esta URL

IP

139[.]59[.]63[.]103

Domain www2.scotia.chile.002l.live is located on IP address << 139.59.63.103 >>

Block start	139.59.0.0
End of block	139.59.255.254
Block size	65535 Domains in block
Block name	DIGITALOCEAN-AP
AS number	14061
Parent block	139.59.0.0 - 139.59.255.255
Organization	DigitalOcean, LLC
Country	SG , Singapore
Host name	no record in reverse zone
Domain count	>= 2 Servers around
Domains	1 002l.live 2 www2.scotia.chile.002l.live

Ilustración 2 IP de origen donde se aloja sitio falso del Banco Itau

Localización

India, Bangalore, Karnataka

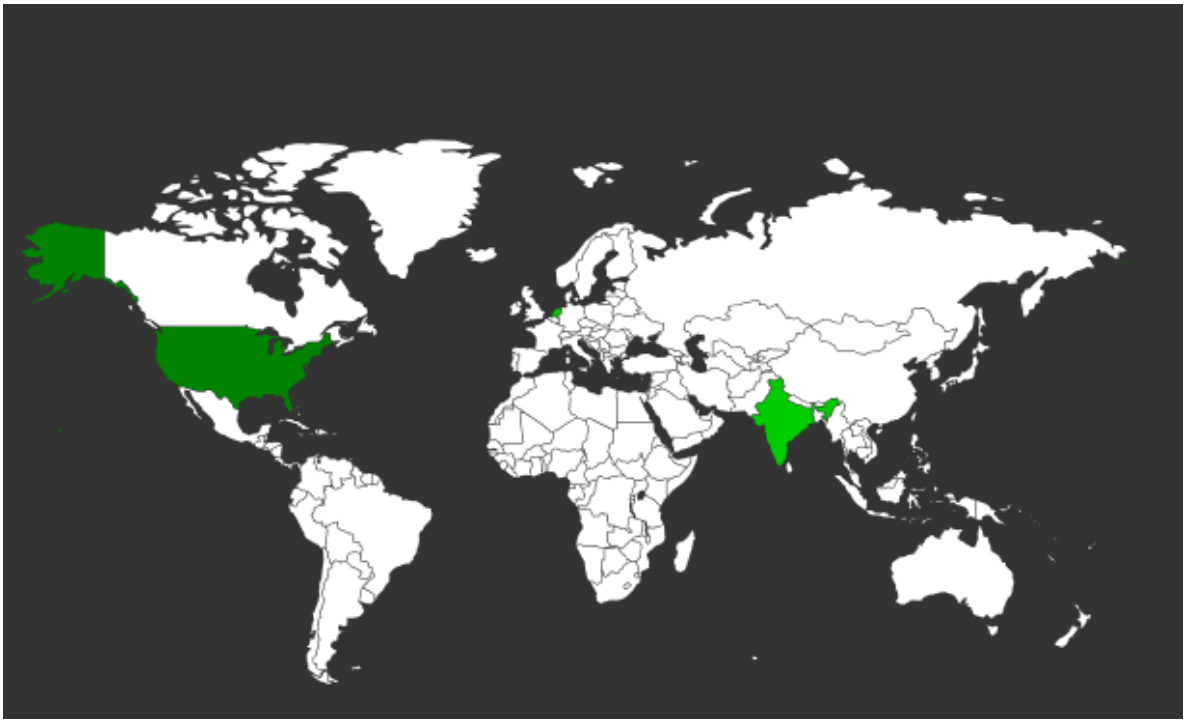
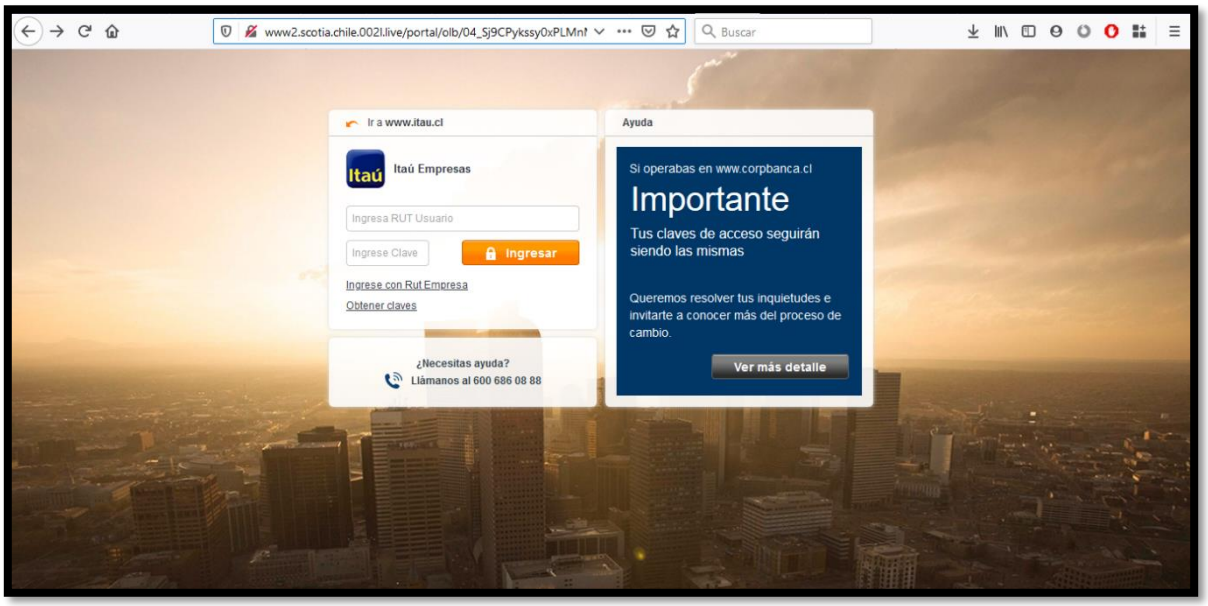


Imagen del sitio



Whois

```
% IANA WHOIS server
% for more information on IANA, visit http://www.iana.org
% This query returned 1 object

refer:        whois.nic.live

domain:       LIVE

organisation: United TLD Holdco Ltd.
address:      One Clarendon Row, Dublin 2, Co. Dublin
address:      Ireland

contact:      administrative
name:         Serina Ness
organisation: Donuts Inc.
address:      Donuts Inc.
address:      5808 Lake Washington Blvd NE, Suite 300
address:      Kirkland, WA 98033
address:      United States
phone:        +1.425.283.8248
fax-no:       +1.425.671.0020
e-mail:       serina@donuts.email

contact:      technical
name:         Ben Levac
organisation: Donuts Inc.
address:      Donuts Inc.
address:      5808 Lake Washington Blvd NE, Suite 300
address:      Kirkland, WA 98033
address:      United States
phone:        +1.425.298.2200
fax-no:       +1.425.671.0020
e-mail:       ben@donuts.email

nserver:      DEMAND.ALPHA.ARIDNS.NET.AU 2001:dcd:1:0:0:0:0:7 37.209.192.7
nserver:      DEMAND.BETA.ARIDNS.NET.AU 2001:dcd:2:0:0:0:0:7 37.209.194.7
nserver:      DEMAND.DELTA.ARIDNS.NET.AU 2001:dcd:4:0:0:0:0:7 37.209.198.7
nserver:      DEMAND.GAMMA.ARIDNS.NET.AU 2001:dcd:3:0:0:0:0:7 37.209.196.7
ds-rdata:     30640 8 1 B1B3A0ED44A1DEA6B8AC93793742680887C6C4AC
ds-rdata:     30640 8 2 C2A186F6BD89AE983EE147EDCE3148A75343EE1F12869ABBCF293388457F495D

whois:        whois.nic.live

status:       ACTIVE
remarks:      Registration information: http://www.donuts.domains/

created:      2015-06-25
changed:      2019-08-01
source:       IANA

Domain not found.

Terms of Use: Donuts Inc. provides this Whois service for information purposes, and to assist persons in obtai
ning information about or related to a domain name registration record. Donuts does not guarantee its accuracy
. Users accessing the Donuts Whois service agree to use the data only for lawful purposes, and under no circum
stances may this data be used to: a) allow, enable, or otherwise support the transmission by e-mail, telephone
, or facsimile of mass unsolicited, commercial advertising or solicitations to entities other than the registr
ar's own existing customers and b) enable high volume, automated, electronic processes that send queries or da
ta to the systems of Donuts or any ICANN-accredited registrar, except as reasonably necessary to register doma
in names or modify existing registrations. When using the Donuts Whois service, please consider the following:
 The Whois service is not a replacement for standard EPP commands to the SRS service. Whois is not considered
authoritative for registered domain objects. The Whois service may be scheduled for downtime during production
 or OT&E maintenance periods. Queries to the Whois services are throttled. If too many queries are received fr
om a single IP address within a specified time, the service will begin to reject further queries for a period
of time to prevent disruption of Whois service access. Abuse of the Whois system through data mining is mitiga
ted by detecting and limiting bulk query access from single sources. Where applicable, the presence of a [Non-
Public Data] tag indicates that such data is not made publicly available due to applicable data privacy laws o
r requirements. Should you wish to contact the registrant, please refer to the Whois records available through
 the registrar URL listed above. Access to non-public data may be provided, upon request, where it can be reas
onably confirmed that the requester holds a specific legitimate interest and a proper legal basis for accessin
g the withheld da
ta. Access to this data can be requested by submitting a request via the form found at https://donuts.domains/
about/policies/whois-layered-access/ Donuts Inc. reserves the right to modify these terms at any time. By subm
itting this query, you agree to abide by this policy.
```

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: 2020.02.16 15:26:26 -03'00'