Alerta de seguridad informática	8FFR-00147-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	10 de Diciembre de 2019
Última revisión	10 de Diciembre 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 tres portales fraudulentos asociados a una IP que suplantan el sitio web oficial de **Banco Itaú**, los que podrían 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

URL Sitio Clonado:
https://bank[.]itau[.]cl[.]wps1-portal[.]info/portal/olb/04_Sj9CPykssy0xPLMnMz0vMAfIjo8ziDVCAo4FTkJGTsYGBu7OJfjhYgb-BpauHYbCBn0WYhZmBo5-xoYungZe7QaCBfhQx-g1wAEey9KMoiMJvfLh-FFgJPh8QMqMgNzQ0wiDTEQCkdp5B[.]php
https[://]itau-empresas-acceso[.]000webhostapp[.]com/user[.]html

Domain wps1-portal.info

wps1-portal / info / Subdomains

record type	TTL	value		
A	7207	159.65.156.55		
NS	172800	ns1.dnsowl.com	Zones on DNS server	104.207.141.138, 198.251.84.16, 185.34.216.159
NS	172800	ns2.dnsowl.com	Zones on DNS server	168.235.75.52, 45.32.237.128, 64.32.22.100
NS	172800	ns3.dnsowl.com	Zones on DNS server	45.63.106.63, 209.141.39.150, 45.63.5.234

SOA	172800	Mname	ns1.dnsowl.com
		Rname	hostmaster.dnsowl.com
		Serial number	1575896416
		Refresh	7200
		Retry	1800
		Expire	1209600
		Minimum TTL	600

Domain 000webhostapp.com

000webhostapp / com / Subdomains

record type	TTL	value		
A	60	153.92.0.100		
NS	900	dns1.000webhost.com	Zones on DNS server	153.92.2.10
NS	900	dns2.000webhost.com	Zones on DNS server	153.92.2.20
MX	3600	1 ASPMX.L.GOOGLE.com		
TXT	3600	google-site-verification=o8fiVtoqn6PtOerlqmBsJ0dDG0-k7szm03Q3-I_nZ10		
TXT	3600	h0xkmxkckcltwjb7v25vhl8c4xngkmst		
TXT	14400	v=spf1 -all		

SOA	900	Mname	dns1.000webhost.com
		Rname	hostmaster.000webhost.com
		Serial number	1
		Refresh	7200
		Retry	900
		Expire	1209600
		Minimum TTL	86400

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

Certificados

Basic Information

Subject DN	CN=bank.itau.cl.wps1-portal.info
Issuer DN	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
Serial	324029804530222372944118781551692844231221
Validity	2019-12-07 17:56:22 **to** 2020-03-06 17:56:22 (90 days, 0:00:00)
Names	bank.itau.cl.wps1-portal.info

Fingerprint

SHA-256	ec76068b83c8f12c713bc5d2f8fe61ceb5923d124dc9c9b855b139829f022e19
SHA-1	707ccc52d1ba78312395c1c0ff2c7e2021fe81a8
MD5	485bf135f077f8ccbacb2ca4df818d77

Public Key

Key Type	2048-bit RSA, e = 65,537 ✔ STRONG
Modulus	b3:d4:8e:a1:99:df:85:4b:68:b1:c3:23:05:cb:cc:d3:c3:09:bb:7d:
SPKI SHA-256	1ec8d97b8c41871841db353a9d4c2b1a1249b8c3b524af9c69d6c1931dbc7037

Criteria	Identity = '000webhostapp.com'; Exclude expired certificates

Certificates

crt.sh ID	Logged At	Not Before	Not After	Issuer Name
1573772898	2019-06-13	2019-06-11	2021-07-10	C=US, O=DigiCert Inc, OU=www.digicert.com, CN=RapidSSL RSA CA 2018
1566039480	2019-06-11	2019-06-11	2021-07-10	C=US, O=DigiCert Inc, OU=www.digicert.com, CN=RapidSSL RSA CA 2018

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

IP

159.65.156.55

153.92.0.100

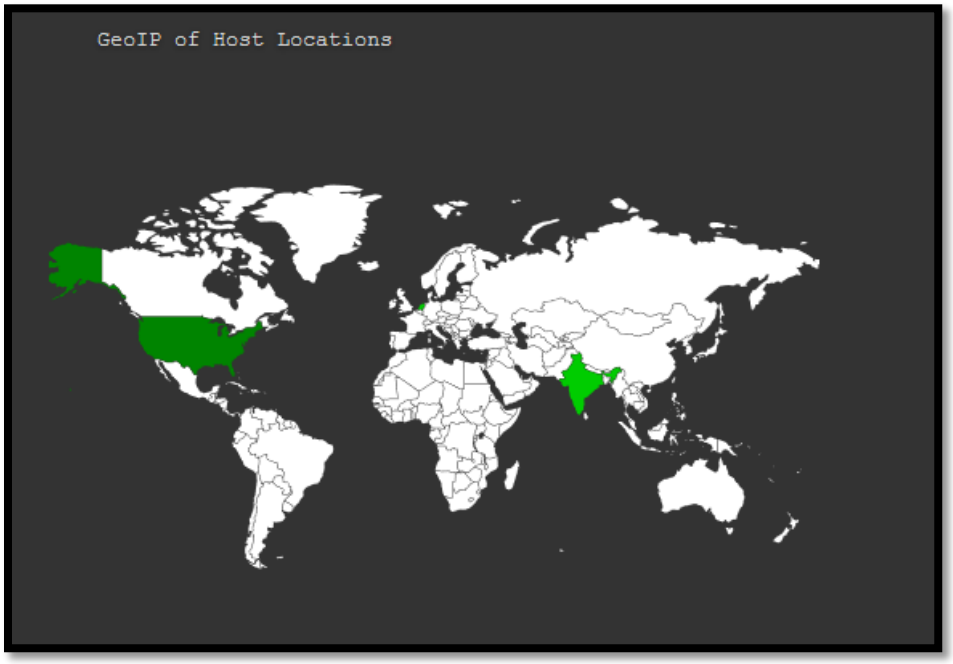
Domain wps1-portal.info is located on IP address << 159.65.156.55 >>	
Block start	159.65.0.0
End of block	159.65.255.255
Block size	65536 Domains in block
Block name	PHS-NET
AS number	14061
Parent block	159.0.0.0 - 159.255.255.255
Organization	PresbyterianHealthcareSys.
City	Dallas
Region/State	Texas
Country	US , United States
Reg. date	1992-03-13
Host name	no record in reverse zone
Domains	1 wps1-portal.info

Domain 000webhostapp.com is located on IP address << 153.92.0.100 >>	
Block start	153.92.0.0
End of block	153.92.15.255
Block size	4096 Domains in block
Block name	HOSTINGER-HOSTING
AS number	204915
Parent block	153.0.0.0 - 153.255.255.255
Organization	ORG-ARTA1-RIPE
City	Charlotte
Region/State	North Carolina
Country	US , United States
Reg. date	1991-09-23
Host name	no record in reverse zone
Domain count	>= 3 Servers around
Domains	1 000webhostapp.com 2 ccshop.comyr.com 3 testing112.comuf.com

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

Localización

Bangalore, Karnataka, India



Ashburn, Virginia, Estados Unidos

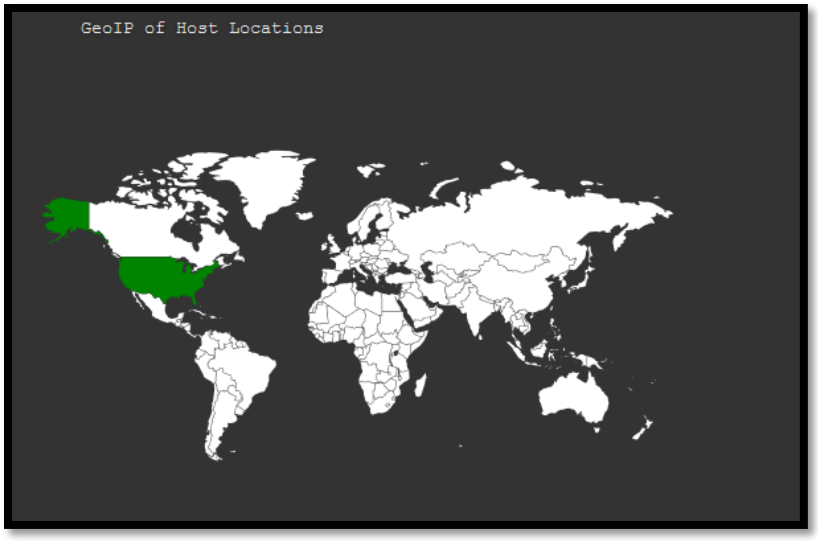
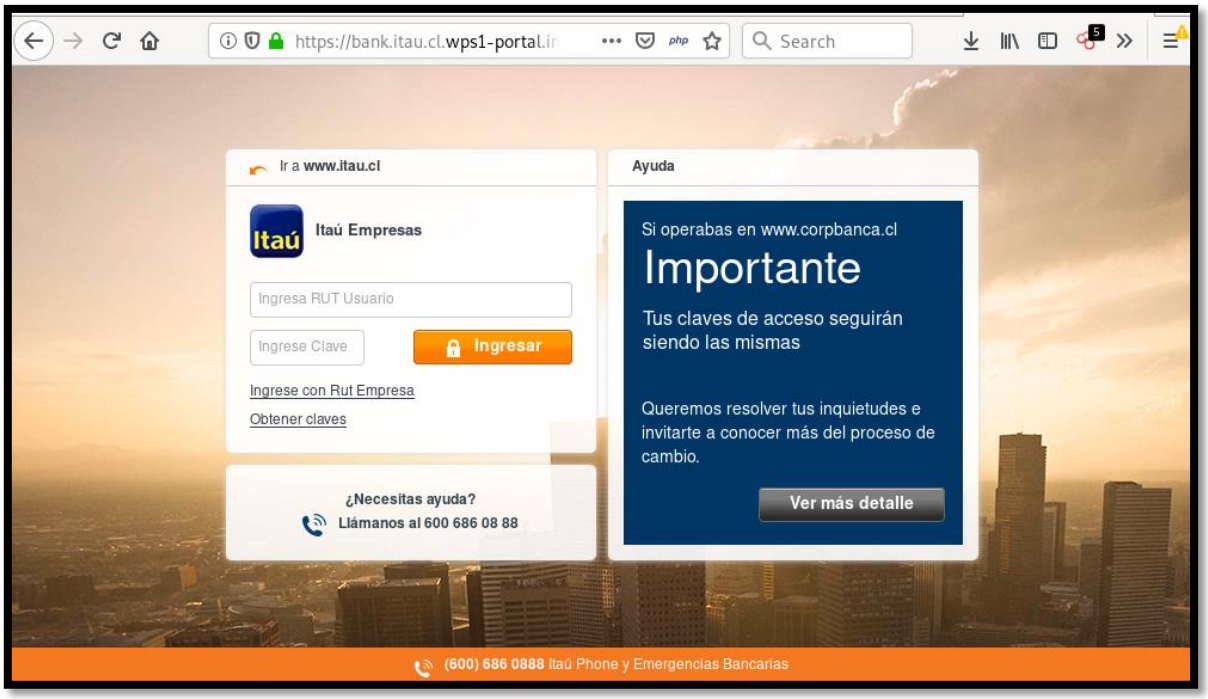
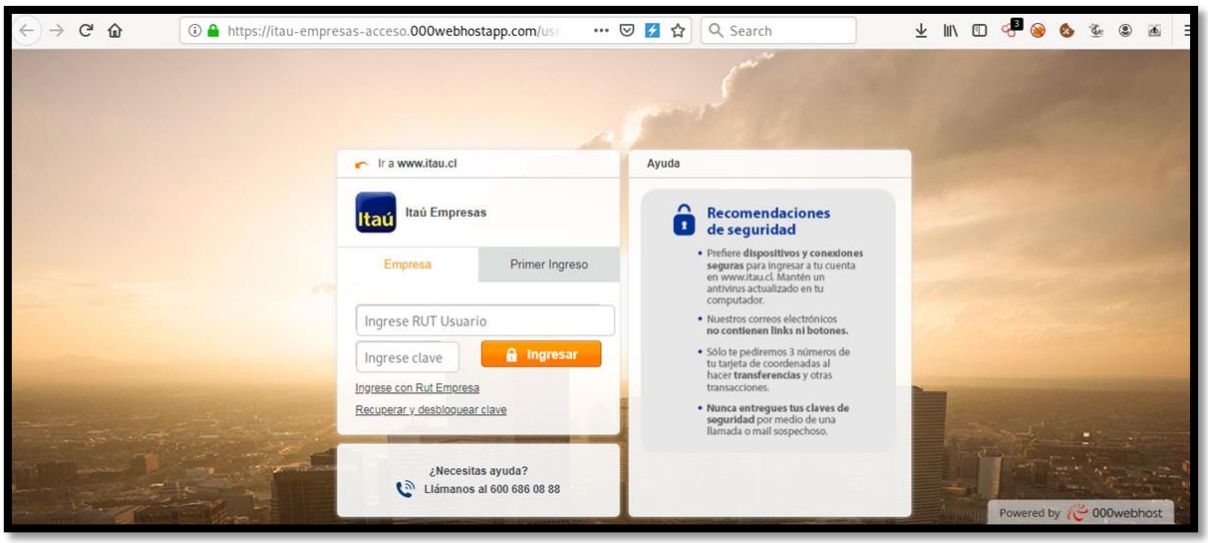


Imagen del sitio





Whois

```
Domain Name: wps1-portal.info
Registry Domain ID: D503300001182527880-LRMS
Registrar WHOIS Server: whois.namesilo.com
Registrar URL: https://www.namesilo.com/
Updated Date: 2019-12-08T07:00:00Z
Creation Date: 2019-12-07T07:00:00Z
Registrar Registration Expiration Date: 2020-12-07T07:00:00Z
Registrar: NameSilo, LLC
Registrar IANA ID: 1479
Registrar Abuse Contact Email: abuse@namesilo.com
Registrar Abuse Contact Phone: +1.4805240066
Domain Status: clientTransferProhibited https://www.icann.org/epp#clientTransferProhibited
Registry Registrant ID:
Registrant Name: Domain Administrator
Registrant Organization: See PrivacyGuardian.org
Registrant Street: 1928 E. Highland Ave. Ste F104 PMB# 255
Registrant City: Phoenix
Registrant State/Province: AZ
Registrant Postal Code: 85016
Registrant Country: US
Registrant Phone: +1.3478717726
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: pw-ddf6bee3ablfe2eac4862d9795ccfcc9@privacyguardian.org
Registry Admin ID:
Admin Name: Domain Administrator
Admin Organization: See PrivacyGuardian.org
Admin Street: 1928 E. Highland Ave. Ste F104 PMB# 255
Admin City: Phoenix
Admin State/Province: AZ
Admin Postal Code: 85016
Admin Country: US
Admin Phone: +1.3478717726
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: pw-ddf6bee3ablfe2eac4862d9795ccfcc9@privacyguardian.org
Registry Tech ID:
Tech Name: Domain Administrator
Tech Organization: See PrivacyGuardian.org
Tech Street: 1928 E. Highland Ave. Ste F104 PMB# 255
Tech City: Phoenix
Tech State/Province: AZ
Tech Postal Code: 85016
Tech Country: US
Tech Phone: +1.3478717726
Tech Phone Ext:
Tech Fax:
Tech Fax Ext:
Tech Email: pw-ddf6bee3ablfe2eac4862d9795ccfcc9@privacyguardian.org
Name Server: NS1.DNSOWL.COM
Name Server: NS2.DNSOWL.COM
Name Server: NS3.DNSOWL.COM
DNSSEC: unsigned
```

```
Domain Name: 000WEBHOSTAPP.COM
Registry Domain ID: 2027404438_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.hostinger.com
Registrar URL: https://www.hostinger.com
Updated Date: 2017-04-05T08:09:44Z
Creation Date: 2016-05-11T13:34:12Z
Registrar Registration Expiration Date: 2022-05-11T13:34:12Z
Registrar: Hostinger, UAB
Registrar IANA ID: 1636
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Registry Registrant ID: Not Available From Registry
Registrant Name: GDPR Masked
Registrant Organization: GDPR Masked
Registrant Street: GDPR Masked GDPR Masked GDPR Masked
Registrant City: GDPR Masked
Registrant State/Province: Larnaka
Registrant Postal Code: GDPR Masked
Registrant Country: CY
Registrant Phone: +GDPR Masked.GDPR Masked
Registrant Phone Ext:
Registrant Fax: +GDPR Masked.GDPR Masked
Registrant Fax Ext:
Registrant Email: gdpr-masking@gdpr-masked.com
Registry Admin ID: Not Available From Registry
Admin Name: GDPR Masked
Admin Organization: GDPR Masked
Admin Street: GDPR Masked GDPR Masked GDPR Masked
Admin City: GDPR Masked
Admin State/Province: Larnaka
Admin Postal Code: GDPR Masked
Admin Country: CY
Admin Phone: +GDPR Masked.GDPR Masked
Admin Phone Ext:
Admin Fax: +GDPR Masked.GDPR Masked
Admin Fax Ext:
Admin Email: gdpr-masking@gdpr-masked.com
Registry Tech ID: Not Available From Registry
Tech Name: GDPR Masked
Tech Organization: GDPR Masked
Tech Street: GDPR Masked GDPR Masked GDPR Masked
Tech City: GDPR Masked
Tech State/Province: Larnaka
Tech Postal Code: GDPR Masked
Tech Country: CY
Tech Phone: +GDPR Masked.GDPR Masked
Tech Phone Ext:
Tech Fax: +GDPR Masked.GDPR Masked
Tech Fax Ext:
Tech Email: gdpr-masking@gdpr-masked.com
Name Server: dns1.000webhost.com
Name Server: dns2.000webhost.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: 2019.12.10 19:06:05 -03'00'