Alerta de seguridad cibernética	8FFR20-00317-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	07 de abril de 2020
Última revisión	07 de abril 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 dos portales fraudulentos asociados a dos IPs que suplantan 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 COMPROMISO

URL
www-itau-cl[.]bluemoonmassage[.]biz
servicioalcliente[.]itaucl-home[.]com

IP
104[.]206[.]225[.]254
195[.]123[.]214[.]221

DOMINIOS DONDE SE ALOJA URL

Domain www-itau-cl.bluemoonmassage.biz

www-itau-cl / bluemoonmassage / biz / Subdomains

record type	TTL	value
A	14400	104.206.225.254

Domain bluemoonmassage.biz

bluemoonmassage / biz / Subdomains

record type	TTL	value		
A	14400	104.206.225.254		
NS	86400	ns1.gooddaddyhosting.com	Zones on DNS server	104.206.226.175
NS	86400	ns2.gooddaddyhosting.com	Zones on DNS server	104.206.226.175
MX	14400	0 bluemoonmassage.biz		
SOA	86400	Mname: ns1.gooddaddyhosting.com Rname: gooddaddyhosting.gmail.com Serial number: 2020040602 Refresh: 3600 Retry: 1800 Expire: 1209600 Minimum TTL: 86400		

Domain servicioalcliente.itaucl-home.com

servicioalcliente / itaucl-home / com / Subdomains

record type	TTL	value
A	14400	195.123.214.221

Domain itaucl-home.com

itaucl-home / com / Subdomains

record type	TTL	value		
A	14400	195.123.214.221		
NS	86400	ns1.itaucl-home.com	Zones on DNS server	195.123.214.221
NS	86400	ns2.itaucl-home.com	Zones on DNS server	195.123.214.221
MX	14400	0 itaucl-home.com		
TXT	14400	v=spf1 +a +mx +ip4:195.123.214.221 ~all		
SOA	86400	Mname: ns1.itaucl-home.com Rname: root.vox.vps.com Serial number: 2020040603 Refresh: 3600 Retry: 1800 Expire: 1209600 Minimum TTL: 86400		

CERTIFICADOS

crt.sh ID	Logged At	Not Before	Not After	Matching Identities	Issuer Name
2672166146	2020-04-06	2020-04-06	2020-07-05	www-itau-cl.bluemoonmassage.biz www.www-itau-cl.bluemoonmassage.biz	C=US, ST=TX, L=Houston, O="cPanel, Inc.", CN="cPanel, Inc. Certification Authority"
2672166088	2020-04-06	2020-04-06	2020-07-05	www-itau-cl.bluemoonmassage.biz www.www-itau-cl.bluemoonmassage.biz	C=US, ST=TX, L=Houston, O="cPanel, Inc.", CN="cPanel, Inc. Certification Authority"

crt.sh ID	Logged At	Not Before	Not After	Matching Identities	Issuer Name
2671424654	2020-04-06	2020-04-05	2020-07-04	servicioalcliente.itaucl-home.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
2671424408	2020-04-06	2020-04-05	2020-07-04	servicioalcliente.itaucl-home.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
2671417342	2020-04-06	2020-04-06	2020-07-05	servicioalcliente.itaucl-home.com www.servicioalcliente.itaucl-home.com	C=US, ST=TX, L=Houston, O="cPanel, Inc.", CN="cPanel, Inc. Certification Authority"
2671417290	2020-04-06	2020-04-06	2020-07-05	servicioalcliente.itaucl-home.com www.servicioalcliente.itaucl-home.com	C=US, ST=TX, L=Houston, O="cPanel, Inc.", CN="cPanel, Inc. Certification Authority"

IP DE ORIGEN DONDE SE ALOJA SITIO

Domain www-itau-cl.bluemoonmassage.biz is located on IP address << 104.206.225.254 >>

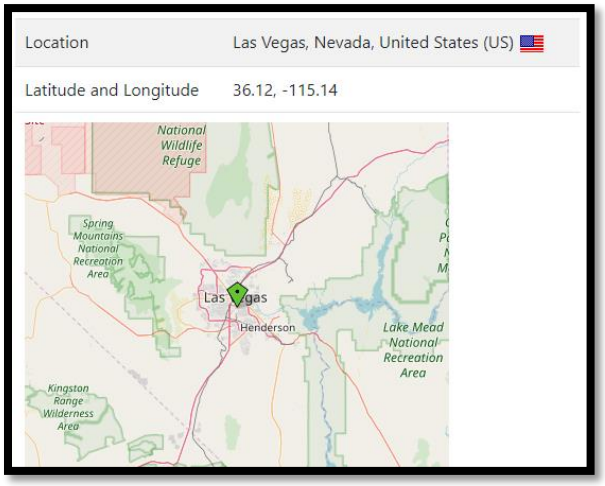
Block start	104.206.0.0
End of block	104.206.255.255
Block size	65536 Domains in block
Block name	EONIX-NET-104-206-0-0-1-BLK-13
AS number	62904
Parent block	104.0.0.0 - 104.255.255.255
Organization	Eonix Corporation

Domain servicioalcliente.itaucl-home.com is located on IP address << 195.123.214.221 >>

Block start	195.123.208.0
End of block	195.123.215.255
Block size	2048 Domains in block
Block name	GF-RIX-NET
AS number	50979
Parent block	195.123.208.0 - 195.123.247.255
Organization	* * As ISP we provide hosting, virtual and dedicated servers. * * Those services are self managed by our customers * therefore, we are not us

LOCALIZACIÓNLIZACIÓN

Las Vegas, Nevada, Estados Unidos



Lituania

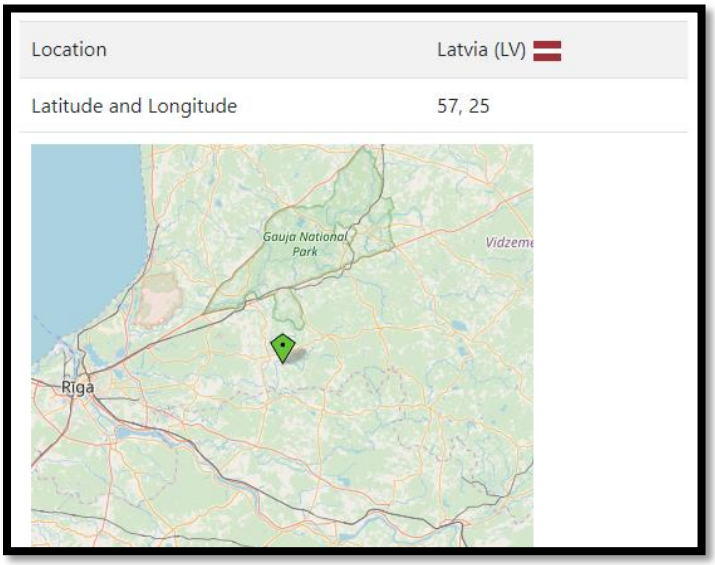
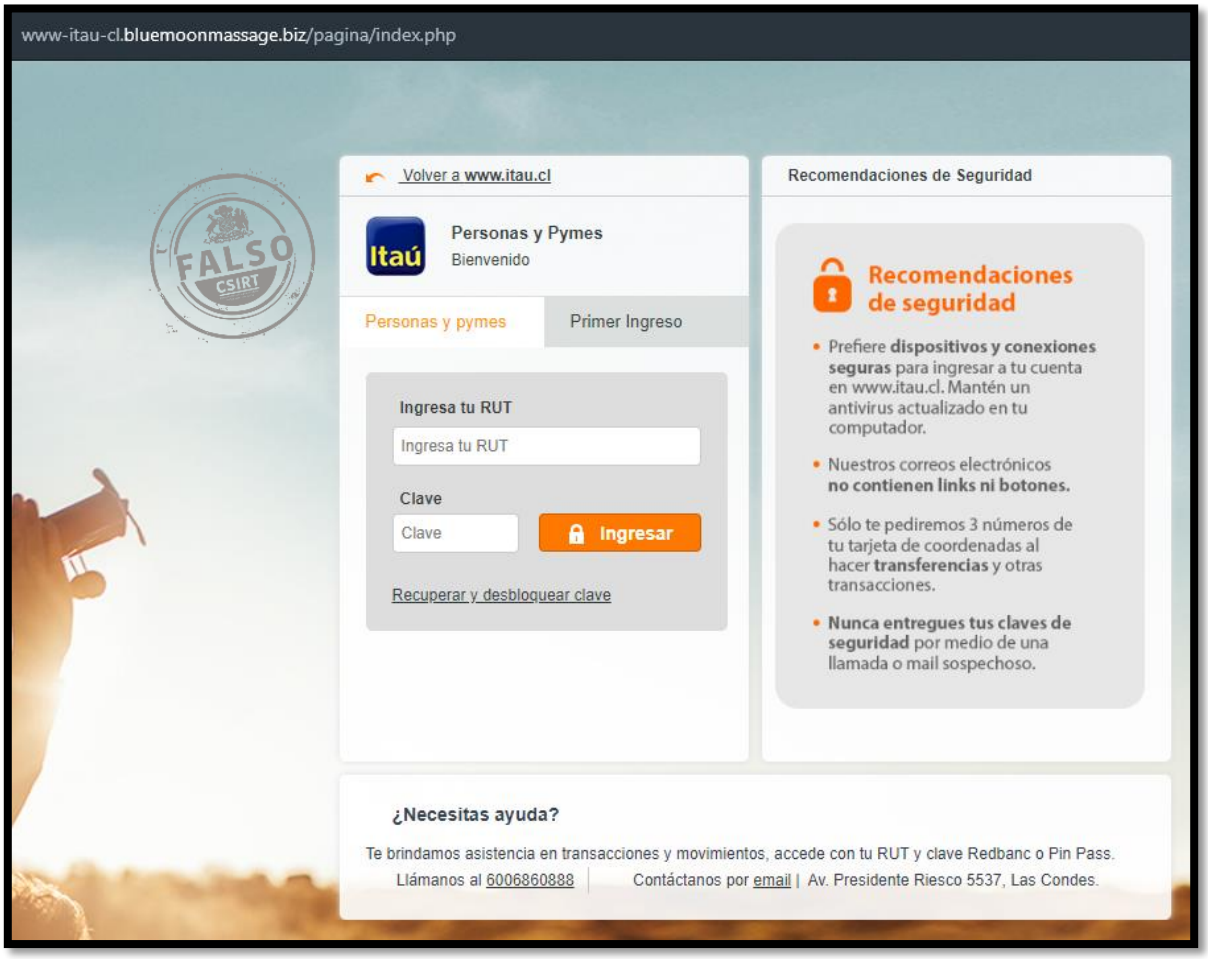
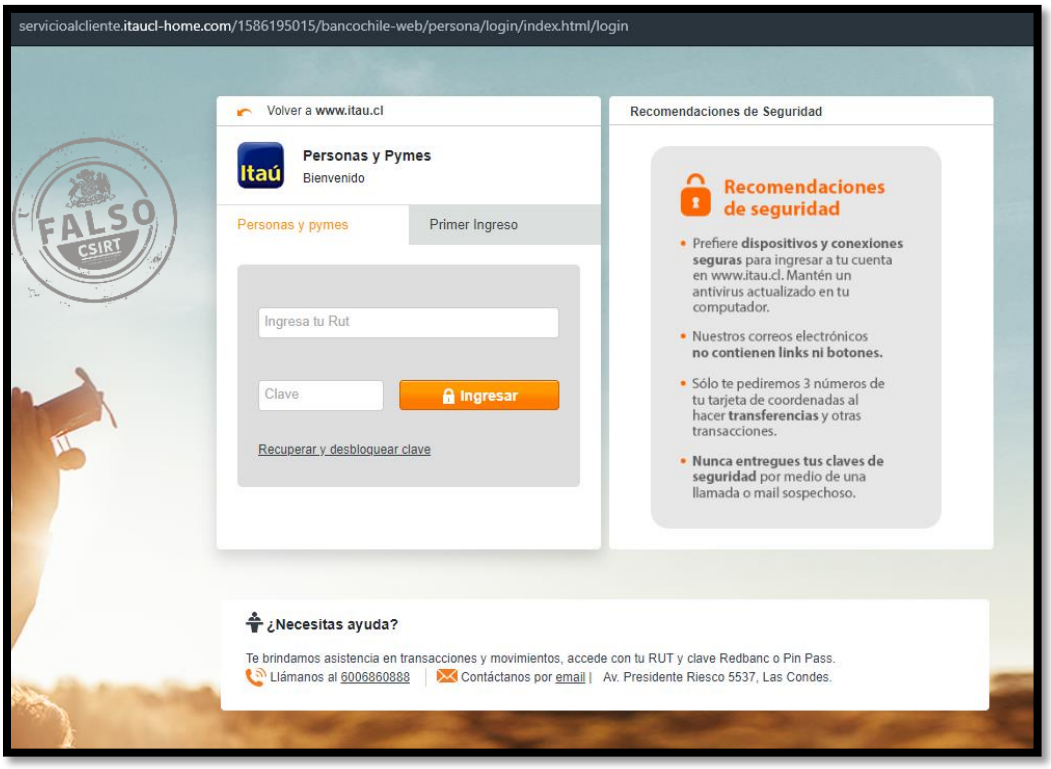
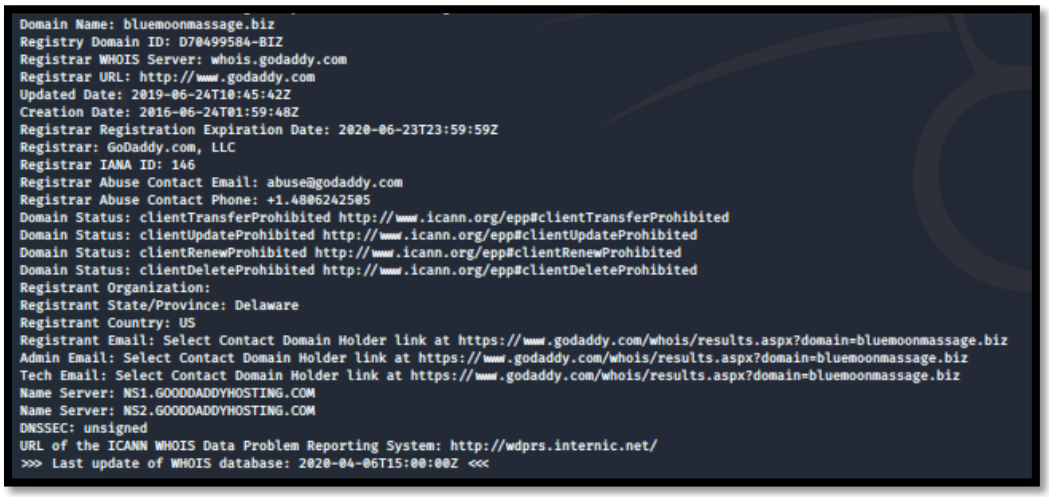


IMAGEN DEL SITIO





WHOIS



```
Domain Name: bluemoonmassage.biz
Registry Domain ID: D70499584-BIZ
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: http://www.godaddy.com
Updated Date: 2019-06-24T10:45:42Z
Creation Date: 2016-06-24T01:59:48Z
Registrar Registration Expiration Date: 2020-06-23T23:59:59Z
Registrar: GoDaddy.com, LLC
Registrar IANA ID: 146
Registrar Abuse Contact Email: abuse@godaddy.com
Registrar Abuse Contact Phone: +1.4806242505
Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited http://www.icann.org/epp#clientUpdateProhibited
Domain Status: clientRenewProhibited http://www.icann.org/epp#clientRenewProhibited
Domain Status: clientDeleteProhibited http://www.icann.org/epp#clientDeleteProhibited
Registrant Organization:
Registrant State/Province: Delaware
Registrant Country: US
Registrant Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=bluemoonmassage.biz
Admin Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=bluemoonmassage.biz
Tech Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=bluemoonmassage.biz
Name Server: NS1.GOODDADDYHOSTING.COM
Name Server: NS2.GOODDADDYHOSTING.COM
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2020-04-06T15:00:00Z <<<
```

```
Domain Name: ITAUCL-HOME.COM
Registry Domain ID: 2511512438_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.domain.com
Registrar URL: www.domain.com
Updated Date: 2020-04-05T23:41:19
Creation Date: 2020-04-05T23:35:09
Registrar Registration Expiration Date: 2021-04-05T23:35:09
Registrar: Domain.com, LLC
Registrar IANA ID: 886
Reseller: Domain.com
Domain Status:
Registry Registrant ID:
Registrant Name: Domain Privacy Service FBO Registrant.
Registrant Organization: Domain Privacy Service FBO Registrant.
Registrant Street: 10 Corporate Drive
Registrant City: Burlington
Registrant State/Province: MA
Registrant Postal Code: 01803
Registrant Country: US
Registrant Phone: +1.6027165339
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: itaucl-home.com@domainprivacygroup.com
Registry Admin ID:
Admin Name: Domain Privacy Service FBO Registrant.
Admin Organization: Domain Privacy Service FBO Registrant.
Admin Street: 10 Corporate Drive
Admin City: Burlington
Admin State/Province: MA
Admin Postal Code: 01803
Admin Country: US
Admin Phone: +1.6027165339
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: itaucl-home.com@domainprivacygroup.com
Registry Tech ID:
Tech Name: Domain Privacy Service FBO Registrant.
Tech Organization: Domain Privacy Service FBO Registrant.
Tech Street: 10 Corporate Drive
Tech City: Burlington
Tech State/Province: MA
Tech Postal Code: 01803
Tech Country: US
Tech Phone: +1.6027165339
Tech Phone Ext:
Tech Fax:
Tech Fax Ext:
Tech Email: itaucl-home.com@domainprivacygroup.com
Name Server: ns2.domain.com
Name Server: ns1.domain.com
DNSSEC: unsigned
Registrar Abuse Contact Email: compliance@domain-inc.net
Registrar Abuse Contact Phone: +1.6027165396
```

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: 2020.04.07 18:40:06 -04'00'