Alerta de seguridad informática	8FFR-00133-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	29 de Noviembre de 2019
Última revisión	29 de Noviembre 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 Itaú**, 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

URL Sitio Clonado:
https[://]itauempresa[.]linkface[.]es/user

Domain linkface.es

linkface / es / Subdomains

record type	TTL	value		
A	3600	217.160.0.38		
NS	86400	ns1095.ui-dns.com	Zones on DNS server	217.160.82.95
NS	86400	ns1097.ui-dns.biz	Zones on DNS server	217.160.81.97
NS	86400	ns1126.ui-dns.org	Zones on DNS server	217.160.83.126
NS	86400	ns1033.ui-dns.de	Zones on DNS server	217.160.80.33
MX	3600	10 mx00.ionos.es		212.227.15.41
MX	3600	10 mx01.ionos.es		217.72.192.67
TXT	60	google-site-verification=3bBCnHLDXsJG3YonGN5HTRLLAh6o43Jl_3NbIssMnUg		

SOA	86400	Mname	ns1126.ui-dns.org
		Rname	hostmaster.1und1.com
		Serial number	2017060103
		Refresh	28800
		Retry	7200
		Expire	604800
		Minimum TTL	600

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

Certificados

Criteria: Identity = 'linkface.es'

Certificates

crt.sh ID	Logged At	Not Before	Not After	Issuer Name
1838969111	2019-09-02	2019-08-26	2020-08-25	C=US, O=DigiCert Inc, OU=www.digicert.com, CN=Encryption Everywhere DV TLS CA - G1
1811420997	2019-08-26	2019-08-26	2020-08-25	C=US, O=DigiCert Inc, OU=www.digicert.com, CN=Encryption Everywhere DV TLS CA - G1

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

IP

217.160.0.38

Domain linkface.es is located on IP address
<< 217.160.0.38 >>

Block start	217.160.0.0
End of block	217.160.1.255
Block size	512 Domains in block
Block name	SCHLUND-CUSTOMERS
AS number	8560
Parent block	217.160.0.0 - 217.160.255.255
Organization	1&1 Internet AG
City	Karlsruhe
Region/State	Baden-Wurttemberg
Country	DE , Germany
Host name	217-160-0-38.elastic-ssl.ui-r.com
Web server	Apache
Domain count	>= 660 Servers around
Domains	1 1717lsv.com 2 247movers.co.uk 3 2procure.co.uk 4 360online.fr 5 3dbimetric.com 6 aak.koeln 7 accademiadelbridge.com 8 acerormigon.com 9 achtungalarm.com

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

Localización

Karlsruhe, Baden-Wurttemberg, Alemania

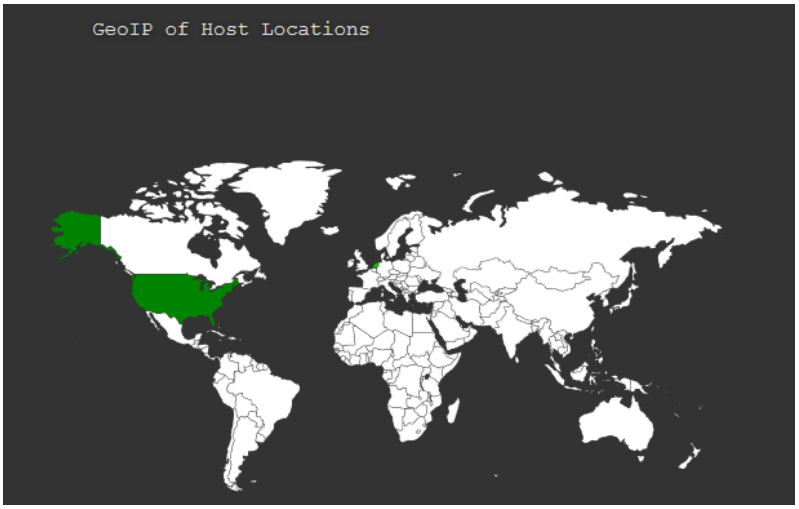
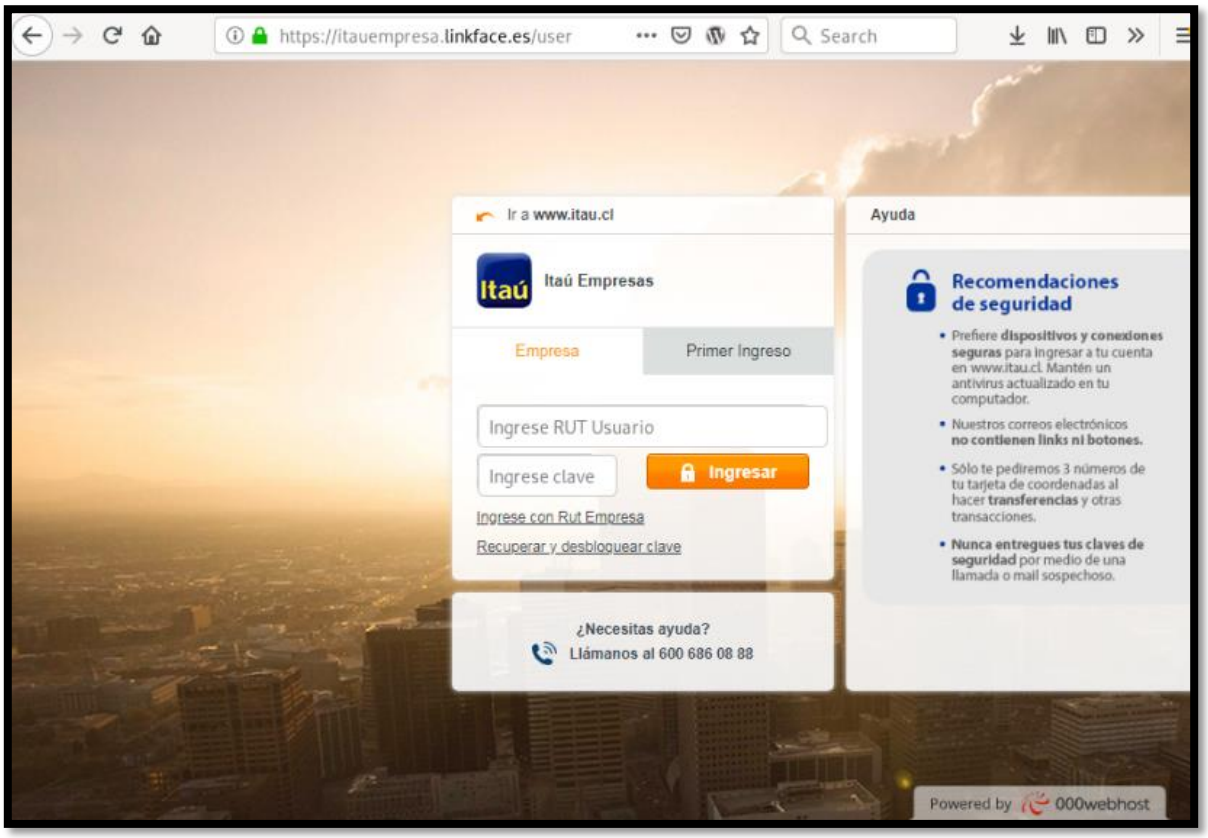


Imagen del sitio



Whois

DATOS DEL TITULAR

Nombre del Dominio	linkface.es
Estado	Activado
Identificador	12C014F-ESNIC-F5
Titular	Maria America Tuya Gonzalez
Fecha de Alta	26-08-2019
Fecha de Caducidad	26-08-2020
Agente Registrador	1&1 IONOS

PERSONA DE CONTACTO ADMINISTRATIVO

Identificador	**12C0150-ESNIC-F5**
Nombre	**Maria America Tuya Gonzalez**

PERSONA DE CONTACTO TECNICO

Identificador	**2A7DD0-ESNIC-F5**
Nombre	**Hostmaster ONEANDONE**

SERVIDORES DNS

Nombre Servidor	**IP**
ns1097.ui-dns.biz	
ns1126.ui-dns.org	
ns1033.ui-dns.de	
ns1095.ui-dns.com	

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: 2019.11.29 09:54:11 -03'00'