| | |
|---|---|
| Alerta de seguridad informática | 8FFR20-00217-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Falsificación de Registros o Identidad |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 13 de febrero de 2020 |
| Última revisión | 13 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 dos portales fraudulentos asociados a una IP que suplanta el sitio web oficial de Banco Estado, 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

payment[.]skytel[.]ie/site/www[.]bancoestado[.]cl/imagenes/comun2008/banca-en-linea-personas[.]html

Redireccionador de URL´s

louairahal[.]net/activacion/cuenta-lgkn/

**Domain payment.skytel.ie**

payment / skytel / ie / Subdomains

| record type | TTL | value |
|---|---|---|
| A | 600 | 160.153.129.228 |

**Domain skytel.ie**

skytel / ie / Subdomains

| record type | TTL | value | | |
|---|---|---|---|---|
| A | 3600 | 160.153.129.228 | | |
| NS | 86400 | auth-dns01.net.skytel.ie | Zones on DNS server | 93.92.8.181 |
| NS | 86400 | auth-sec01.ibn.ie | Zones on DNS server | 46.182.8.9 |
| NS | 86400 | auth-dns02.net.skytel.ie | Zones on DNS server | 93.92.8.197 |
| MX | 3600 | 10 mail.blacknight.com | | 81.17.254.9 |
| TXT | 86400 | v=spf1 a ipv4:160.153.153.164 include:spf.blacknight.com -all | | |
| TXT | 3600 | MS=ms51403051 | | |
| SOA | 86400 | Mname: auth-dns01.net.skytel.ie<br>Rname: hostmaster.net.skytel.ie<br>Serial number: 1578643884<br>Refresh: 86400<br>Retry: 600<br>Expire: 2419200<br>Minimum TTL: 3600 | | |

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

Certificados

| | |
|---|---|
| **Subject DN** | OU=Domain Control Validated, CN=payment.skytel.ie |
| **Issuer DN** | C=US, ST=Arizona, L=Scottsdale, O=GoDaddy.com, Inc., OU=http://certs.godaddy.com/repository/, CN=Go Daddy Secure Certificate Authority - G2 |
| **Serial** | 12778041407687412620 |
| **Validity** | 2019-06-24 13:48:24 **to** 2021-09-19 13:48:24 (818 days, 0:00:00) |
| **Names** | payment.skytel.ie<br>www.payment.skytel.ie |

*Ilustración 2 Certificado Utilizado en Url del sitio Falso del Banco Estado*

IP

160[.]153[.]129[.]228

**Domain payment.skytel.ie is located on IP address << 160.153.129.228 >>**

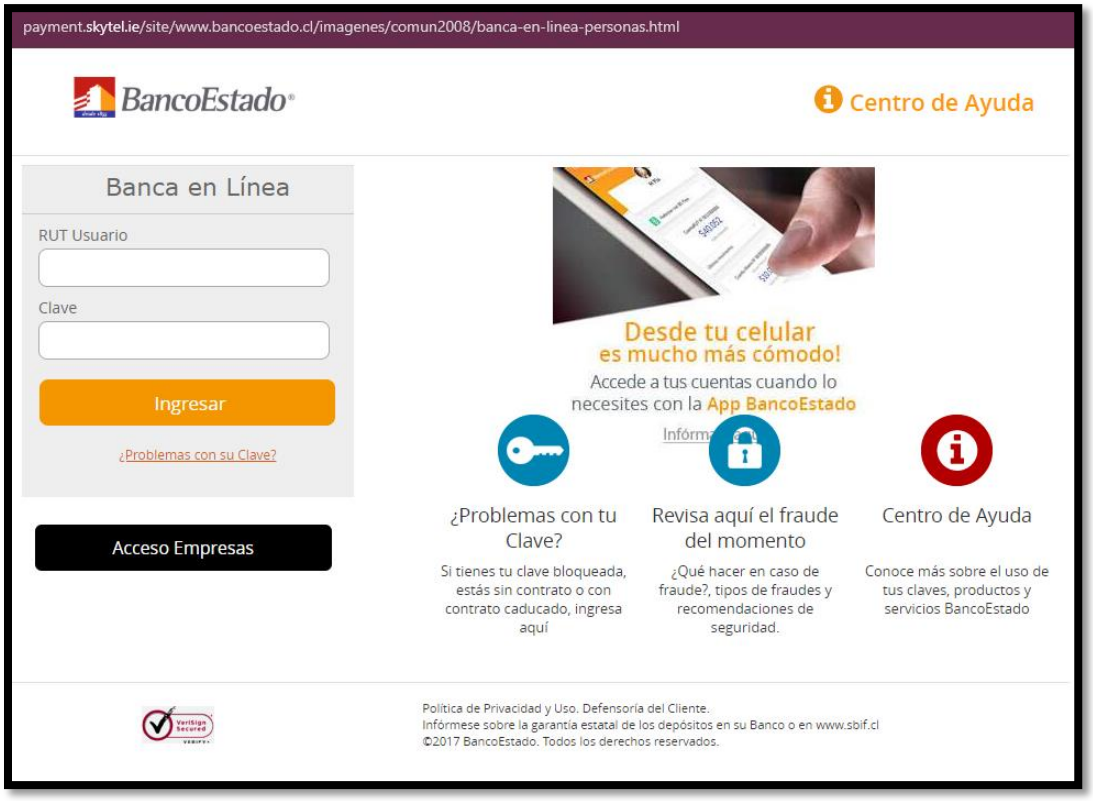
| | |
|---|---|
| **Block start** | 160.153.0.0 |
| **End of block** | 160.153.255.255 |
| **Block size** | 65536 Domains in block |
| **Block name** | GO-DADDY-COM-LLC |
| **AS number** | 21501 |
| **Parent block** | 160.0.0.0 - 160.255.255.255 |
| **Organization** | GoDaddy.com, LLC |
| **City** | Scottsdale |
| **Region/State** | Arizona |
| **Country** | US , United States |
| **Reg. date** | 2011-09-01 |
| **Host name** | ip-160-153-129-228.ip.secureserver.net |
| **Web server** | Apache/2.4.23 |

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

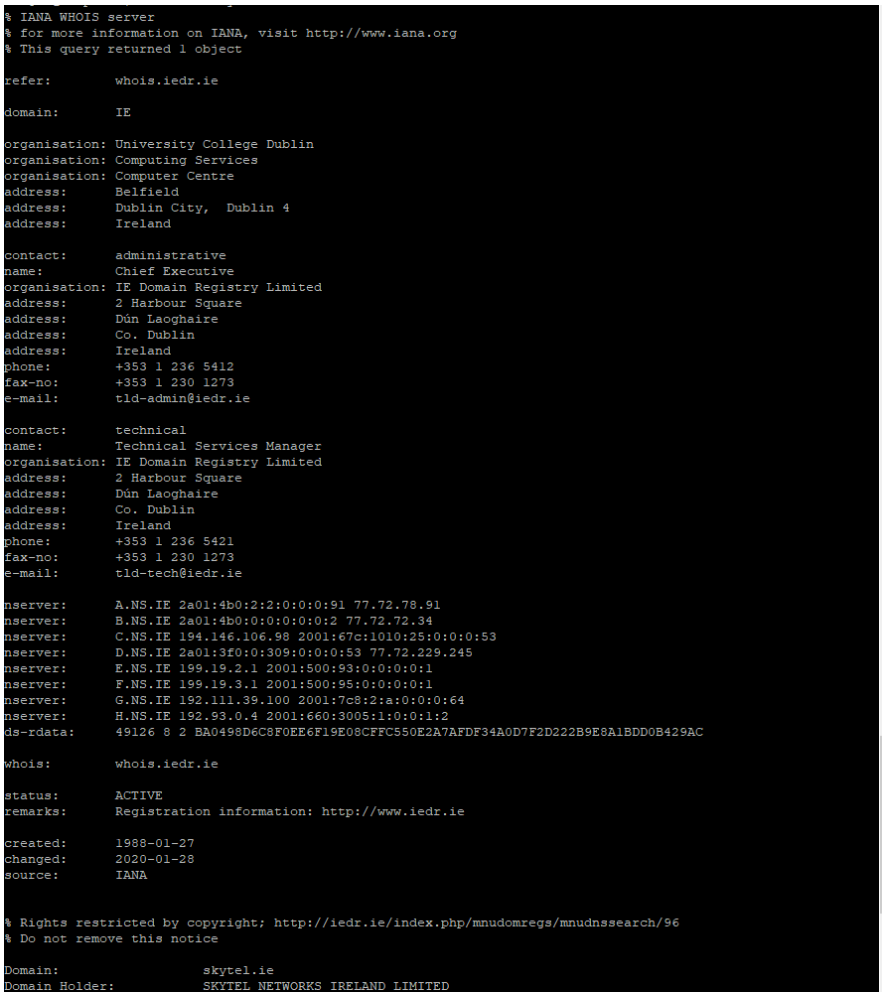
Localización

Scottsdale, Arizona, United States of America

Imagen del sitio



## Whois



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

refer:        whois.iedr.ie

domain:       IE

organisation: University College Dublin
organisation: Computing Services
organisation: Computer Centre
address:      Belfield
address:      Dublin City,  Dublin 4
address:      Ireland

contact:      administrative
name:         Chief Executive
organisation: IE Domain Registry Limited
address:      2 Harbour Square
address:      Dún Laoghaire
address:      Co. Dublin
address:      Ireland
phone:        +353 1 236 5412
fax-no:       +353 1 230 1273
e-mail:       tld-admin@iedr.ie

contact:      technical
name:         Technical Services Manager
organisation: IE Domain Registry Limited
address:      2 Harbour Square
address:      Dún Laoghaire
address:      Co. Dublin
address:      Ireland
phone:        +353 1 236 5421
fax-no:       +353 1 230 1273
e-mail:       tld-tech@iedr.ie

nserver:      A.NS.IE 2a01:4b0:2:2:0:0:0:91 77.72.78.91
nserver:      B.NS.IE 2a01:4b0:0:0:0:0:0:2 77.72.72.34
nserver:      C.NS.IE 194.146.106.98 2001:67c:1010:25:0:0:0:53
nserver:      D.NS.IE 2a01:3f0:0:309:0:0:0:53 77.72.229.245
nserver:      E.NS.IE 199.19.2.1 2001:500:93:0:0:0:0:1
nserver:      F.NS.IE 199.19.3.1 2001:500:95:0:0:0:0:1
nserver:      G.NS.IE 192.111.39.100 2001:7c8:2:a:0:0:0:64
nserver:      H.NS.IE 192.93.0.4 2001:660:3005:1:0:0:1:2
ds-rdata:     49126 8 2 BA0498D6C8F0EE6F19E08CFFC550E2A7AFDF34A0D7F2D222B9E8A1BDD0B429AC

whois:        whois.iedr.ie

status:       ACTIVE
remarks:      Registration information: http://www.iedr.ie

created:      1988-01-27
changed:      2020-01-28
source:       IANA


% Rights restricted by copyright; http://iedr.ie/index.php/mnudomregs/mnudnssearch/96
% Do not remove this notice

Domain:                 skytel.ie
Domain Holder:          SKYTEL NETWORKS IRELAND LIMITED
```

## 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: 2020.02.13 15:45:29 -03'00'