Alerta de seguridad informática	8FFR-00109-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 de Noviembre de 2019
Última revisión	13 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 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

URL´s

https[://]estadocl[.]logosbanking[.]com/index_2[.]html

Domain logosbanking.com

logosbanking / com / Subdomains

record type	TTL	value		
A	3600	217.160.0.178		
NS	86400	ns1076.ui-dns.org	Zones on DNS server	217.160.83.76
NS	86400	ns1082.ui-dns.biz	Zones on DNS server	217.160.81.82
NS	86400	ns1032.ui-dns.com	Zones on DNS server	217.160.82.32
NS	86400	ns1017.ui-dns.de	Zones on DNS server	217.160.80.17
MX	3600	10 mx01.ionos.es		217.72.192.67
MX	3600	10 mx00.ionos.es		212.227.15.41
SOA	86400	Mname	ns1076.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 Estado, Falso y DNS que utiliza

Certificado

Criteria: Identity = 'logosbanking.com'

Certificates

crt.sh ID	Logged At	Not Before	Not After	Issuer Name
1909794709	2019-09-21	2019-09-12	2020-09-11	C=US, O=DigiCert Inc, OU=www.digicert.com, CN=Encryption Everywhere DV TLS CA - G1
1876275795	2019-09-12	2019-09-12	2020-09-11	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 Estado

IP´s

217[.]160[.]0[.]178

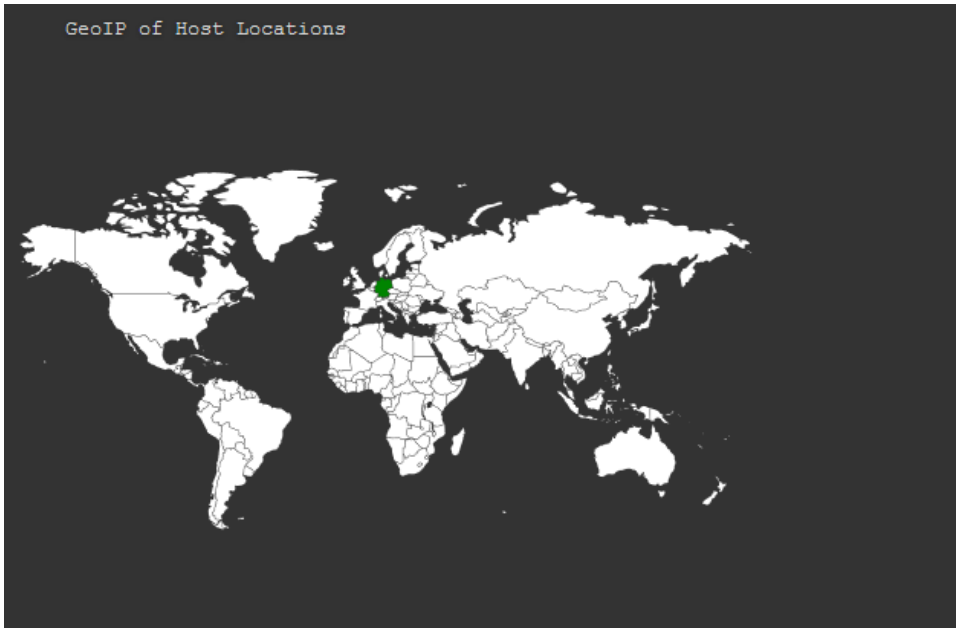
Domain logosbanking.com is located on IP address
<< 217.160.0.178 >>

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	217-160-0-178.elastic-ssl.ui-r.com
Web server	nginx
Domain count	>= 549 Servers around
Domains	401 landing-page.es 402 langenohl.net 403 langenohl.online 404 ldshop.de 405 led-striplighting.com 406 ledessusdupanier.eu 407 lefri-beauty.com 408 lejardindesbeauxarts.com 409 leprachaunmusic.com 410 leshuilesfrancaises.fr 411 lesrppc.com

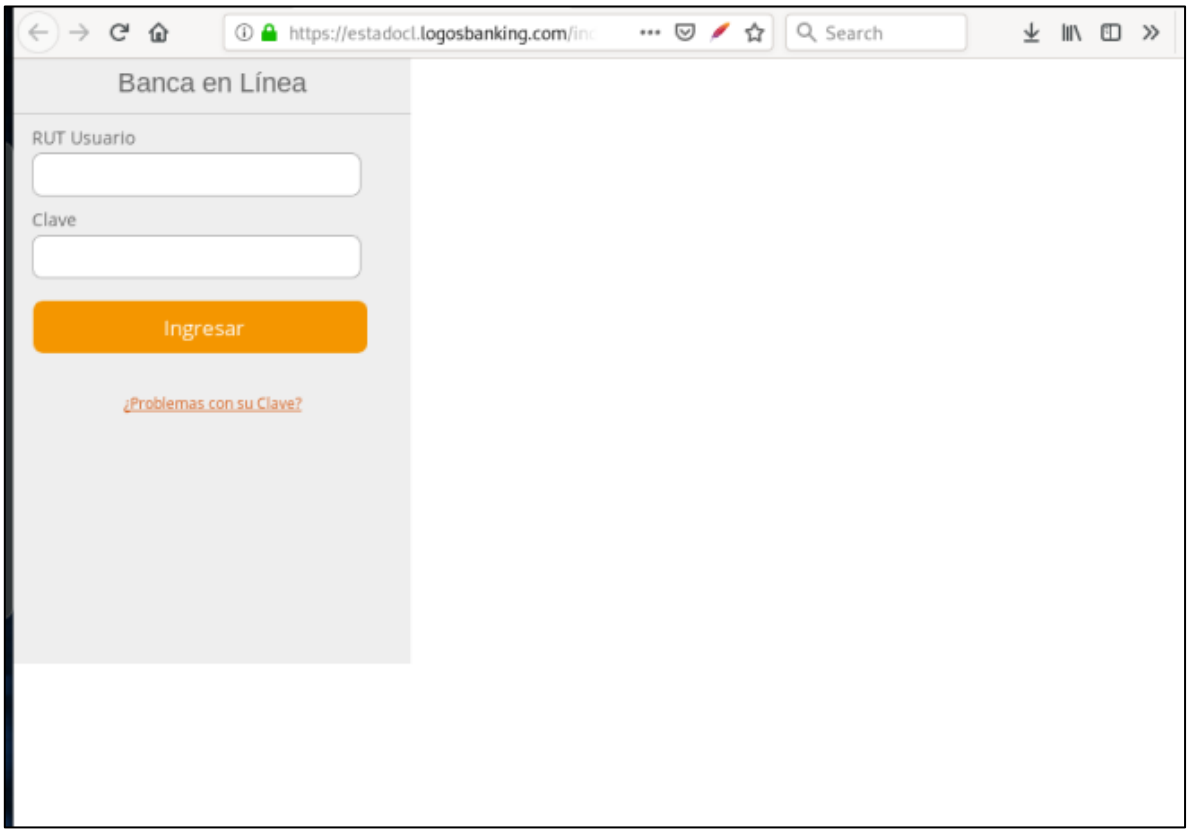
Ilustración 3 Ip de Origen donde se aloja Sitio Falso del Banco Estado

Localización

Karlsruhe, Baden-Wurttemberg, Alemania



Imagen


https://estadocl.logosbanking.com/
Search
Banca en Línea
RUT Usuario
Clave
Ingresar
¿Problemas con su Clave?

Whois

```
soc@ITQ-ivps3:~$ whois -h whois.ionos.com logosbanking.com
Domain Name: logosbanking.com
Registry Domain ID: 2432472277_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.ionos.com
Registrar URL: http://ionos.com
Updated Date: 2019-09-12T10:27:42.000Z
Creation Date: 2019-09-12T10:27:38.000Z
Registrar Registration Expiration Date: 2020-09-12T10:27:38.000Z
Registrar: 1&1 IONOS SE
Registrar IANA ID: 83
Registrar Abuse Contact Email: abuse@ionos.com
Registrar Abuse Contact Phone: +1.8774612631
Reseller:
Domain Status: clientTransferProhibited https://www.icann.org/epp#clientTransferProhibited
Domain Status: addPeriod https://www.icann.org/epp#addPeriod
Registry Registrant ID:
Registrant Name: 1&1 Internet Limited
Registrant Organization: 1&1 Internet Limited
Registrant Street: Discovery House
Registrant Street: 154 Southgate Street
Registrant City: Gloucester
Registrant State/Province: GLS
Registrant Postal Code: GL1 2EX
Registrant Country: GB
Registrant Phone: +44.3333365691
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: privacy@land1.es
Registry Admin ID: REDACTED FOR PRIVACY
Admin Name: REDACTED FOR PRIVACY
Admin Organization: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
Admin City: REDACTED FOR PRIVACY
Admin State/Province: REDACTED FOR PRIVACY
Admin Postal Code: REDACTED FOR PRIVACY
Admin Country: REDACTED FOR PRIVACY
Admin Phone: REDACTED FOR PRIVACY
Admin Phone Ext: REDACTED FOR PRIVACY
Admin Fax: REDACTED FOR PRIVACY
Admin Fax Ext: REDACTED FOR PRIVACY
Admin Email: privacy@land1.es
Registry Tech ID: REDACTED FOR PRIVACY
Tech Name: REDACTED FOR PRIVACY
Tech Organization: REDACTED FOR PRIVACY
Tech Street: REDACTED FOR PRIVACY
Tech City: REDACTED FOR PRIVACY
Tech State/Province: REDACTED FOR PRIVACY
Tech Postal Code: REDACTED FOR PRIVACY
Tech Country: REDACTED FOR PRIVACY
Tech Phone: REDACTED FOR PRIVACY
Tech Phone Ext: REDACTED FOR PRIVACY
Tech Fax: REDACTED FOR PRIVACY
Tech Fax Ext: REDACTED FOR PRIVACY
Tech Email: privacy@land1.es
Nameserver: ns1017.ui-dns.de
Nameserver: ns1076.ui-dns.org
Nameserver: ns1082.ui-dns.biz
Nameserver: ns1032.ui-dns.com
DNSSEC: Unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
```

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: 2019.11.13 13:05:02 -03'00'