Alerta de seguridad informática	8FFR20-00173-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	05 de enero de 2020
Última revisión	05 de enero 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 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
pollachilena[.]servicioalclientes[.]online

Domain servicioalclientes.online

servicioalclientes / online / Subdomains

record type	TTL	value		
A	14400	194.59.164.186		
NS	86400	ns1.dns-parking.com	Zones on DNS server	162.159.24.201
NS	86400	ns2.dns-parking.com	Zones on DNS server	162.159.25.42
MX	14400	10 mx2.hostinger.com		185.224.136.6, 145.14.159.241
MX	14400	10 mx1.hostinger.com		185.224.136.6, 145.14.159.241
TXT	14400	v=spf1 include:spf.mx.hostinger.com include:relay.mailchannels.net ~all		
SOA	3600	Mname: ns1.dns-parking.com Rname: dns.hostinger.com Serial number: 2020010307 Refresh: 10000 Retry: 2400 Expire: 604800 Minimum TTL: 3600		

Ilustración 1 Dominio donde se Aloja Url de BANCO ESTADO, Falso y DNS que utiliza

Certificados

Subject DN	CN=pollachilena.servicioalclientes.online
Issuer DN	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
Serial	380255840679583644107098413900884558941928
Validity	2020-01-03 09:12:02 **to** 2020-04-02 09:12:02 (90 days, 0:00:00)
Names	pollachilena.servicioalclientes.online

Ilustración 2 Certificado Utilizado en Url del sitio Falso de BANCO ESTADO

Localización
Singapur, Singapur.

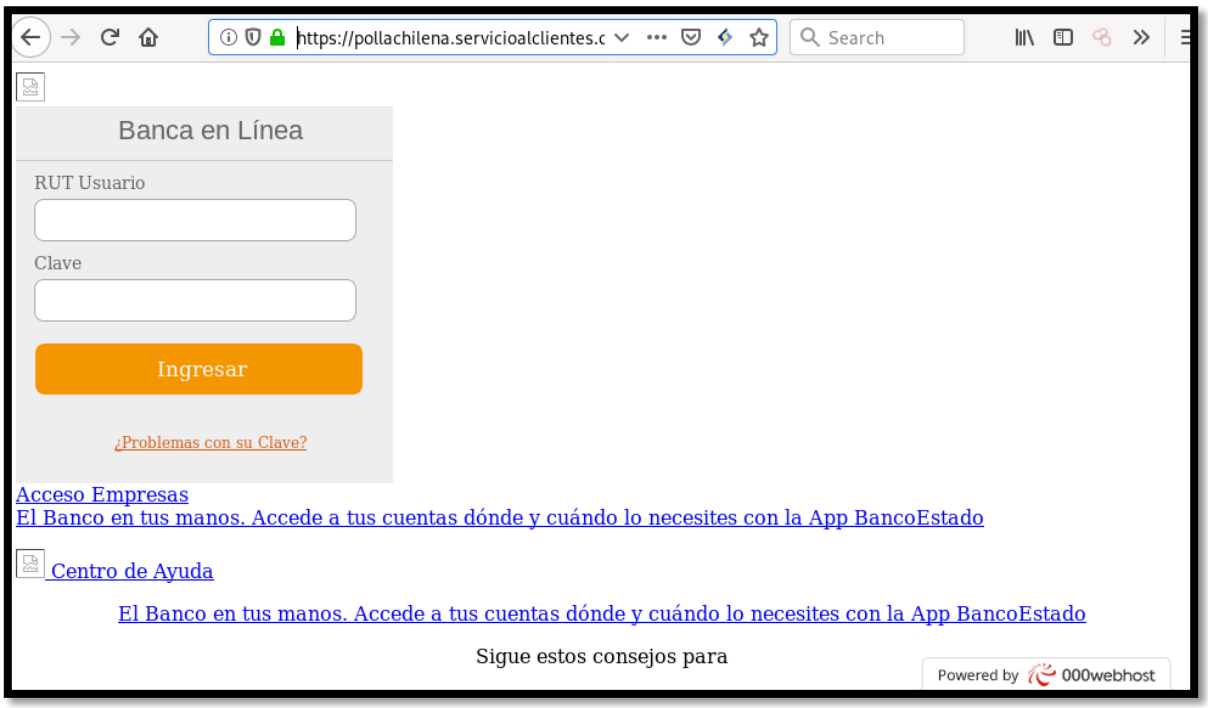
IP
194[.]59[.]164[.]186

Domain servicioalclientes.online is located on IP address << 194.59.164.186 >>

Block start	194.59.164.0
End of block	194.59.165.255
Block size	512 Domains in block
Block name	HOSTINGER-HOSTING-20180311
AS number	47583
Parent block	194.59.164.0 - 194.59.167.255
Organization	ORG-HIL7-RIPE
City	Singapore
Region/State	Singapore
Country	SG , Singapore
Host name	no record in reverse zone
Domains	1 servicioalclientes.online

Ilustración 3 Ip de Origen donde se aloja Sitio Falso de BANCO ESTADO

Imagen del sitio



Whois

```
~$ whois servicioalclientes.online
Domain Name: SERVICIOALCLIENTES.ONLINE
Registry Domain ID: D158272921-CNIC
Registrar WHOIS Server: whois.hostinger.com
Registrar URL:
Updated Date: 2020-01-03T06:51:50.0Z
Creation Date: 2020-01-03T06:51:49.0Z
Registry Expiry Date: 2021-01-03T23:59:59.0Z
Registrar: Hostinger, UAB
Registrar IANA ID: 1636
Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: addPeriod https://icann.org/epp#addPeriod
Registrant Organization: eduardo mesa
Registrant State/Province: metropolitana
Registrant Country: CL
Registrant Email: Please query the RDDS service of the Registrar of Record identified in this output for infor
mation on how to contact the Registrant, Admin, or Tech contact of the queried domain name.
Admin Email: Please query the RDDS service of the Registrar of Record identified in this output for informatio
n on how to contact the Registrant, Admin, or Tech contact of the queried domain name.
Tech Email: Please query the RDDS service of the Registrar of Record identified in this output for information
 on how to contact the Registrant, Admin, or Tech contact of the queried domain name.
Name Server: NS2.DNS-PARKING.COM
Name Server: NS1.DNS-PARKING.COM
DNSSEC: unsigned
Billing Email: Please query the RDDS service of the Registrar of Record identified in this output for informat
ion on how to contact the Registrant, Admin, or Tech contact of the queried domain name.
Registrar Abuse Contact Email: domains@hostinger.com
Registrar Abuse Contact Phone: +370.68424669
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of WHOIS database: 2020-01-03T13:25:32.0Z <<<

For more information on Whois status codes, please visit https://icann.org/epp

>>> IMPORTANT INFORMATION ABOUT THE DEPLOYMENT OF RDAP: please visit
https://www.centralnic.com/support/rdap <<<

The Whois and RDAP services are provided by CentralNic, and contain
information pertaining to Internet domain names registered by our
our customers. By using this service you are agreeing (1) not to use any
information presented here for any purpose other than determining
ownership of domain names, (2) not to store or reproduce this data in
any way, (3) not to use any high-volume, automated, electronic processes
to obtain data from this service. Abuse of this service is monitored and
actions in contravention of these terms will result in being permanently
blacklisted. All data is (c) CentralNic Ltd (https://www.centralnic.com)

Access to the Whois and RDAP services is rate limited. For more
information, visit https://registrar-console.centralnic.com/pub/whois_guidance.
```

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.