Alerta de seguridad informática	8FFR20-00214-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	11 de Febrero de 2020
Última revisión	11 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 del 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

www1[.]bankestado[.]cl[.]tadcl[.]info
www1[.]bankestado[.]cl[.]tadcl[.]info/imagenes/comun2008/banca-en-linea-personas[.]php?html

Domain www1.bankestado.cl.tadcl.info

www1 / bankestado / cl / tadcl / info / Subdomains

record type	TTL	value
A	7207	139.59.12.62

Domain tadcl.info

tadcl / info / Subdomains

record type	TTL	value		
A	7207	139.59.12.62		
NS	172800	ns1.dnsowl.com	Zones on DNS server	104.207.141.138, 198.251.84.16, 185.34.216.159
NS	172800	ns2.dnsowl.com	Zones on DNS server	64.32.22.100, 168.235.75.52, 45.32.237.128
NS	172800	ns3.dnsowl.com	Zones on DNS server	45.63.106.63, 45.63.5.234, 209.141.39.150
SOA	172800	Mname	ns1.dnsowl.com	
		Rname	hostmaster.dnsowl.com	
		Serial number	1581359454	
		Refresh	7200	
		Retry	1800	
		Expire	1209600	
		Minimum TTL	600	

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

Certificados

Subject DN	CN=www1.bankestado.cl.tadcl.info
Issuer DN	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
Serial	271220328318462616384519775011495817395317
Validity	2020-02-08 00:06:21 **to** 2020-05-08 00:06:21 (90 days, 0:00:00)
Names	www1.bankestado.cl.tadcl.info

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

IP

139[.]59[.]12[.]62

Domain www1.bankestado.cl.tadcl.info is located on IP address << 139.59.12.62 >>	
Block start	139.59.0.0
End of block	139.59.255.254
Block size	65535 Domains in block
Block name	DIGITALOCEAN-AP
AS number	14061
Parent block	139.59.0.0 - 139.59.255.255
Organization	DigitalOcean, LLC
Country	SG , Singapore
Host name	no record in reverse zone

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

Localización

India Bangalore, Karnataka

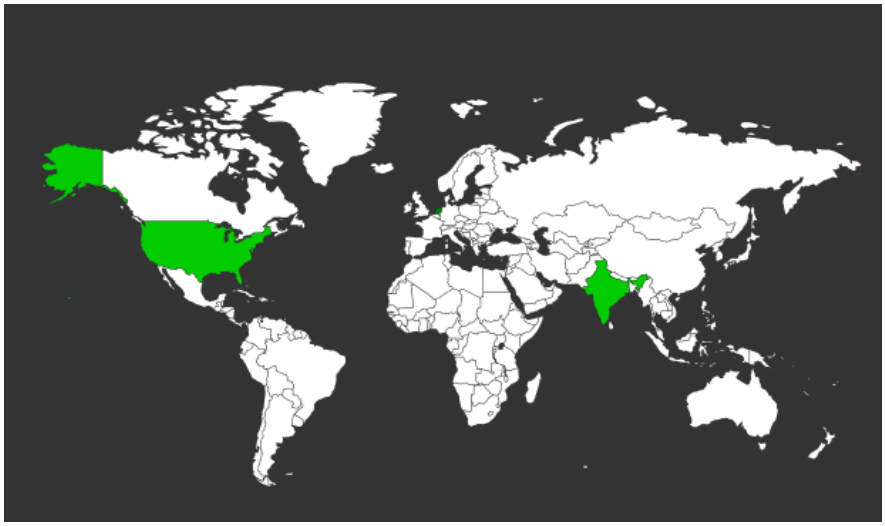

Imagen del sitio

Whois

```
Domain Name: TADCL.INFO
Registry Domain ID: D503300001182978145-LRMS
Registrar WHOIS Server: whois.namesilo.com
Registrar URL: http://www.namesilo.com
Updated Date: 2020-01-30T02:30:48Z
Creation Date: 2020-01-30T02:29:23Z
Registry Expiry Date: 2021-01-30T02:29:23Z
Registrar Registration Expiration Date:
Registrar: Namesilo, LLC
Registrar IANA ID: 1479
Registrar Abuse Contact Email: abuse@namesilo.com
Registrar Abuse Contact Phone: +1.4805240066
Reseller:
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
Registrant Organization: See PrivacyGuardian.org
Registrant State/Province: AZ
Registrant Country: US
Name Server: NS3.DNSOWL.COM
Name Server: NS1.DNSOWL.COM
Name Server: NS2.DNSOWL.COM
DNSSEC: unsigned
```

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: 2020.02.11 13:29:41 -03'00'