Alerta de seguridad cibernética	8FFR20-00443-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	09 de Junio de 2020
Última revisión	09 de Junio 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 compromiso

URL
https[:]//www.bancoestado.cl.personas.banca.en.linea.suzyxs[.]online/wpt/

IP
54[.]153[.]28[.]78

Dominio donde se aloja URL

Domain suzyxs.online

suzyxs / online / Subdomains

record type	TTL	value		
A	600	50.63.202.33		
NS	3600	ns41.domaincontrol.com	Zones on DNS server	97.74.100.21
NS	3600	ns42.domaincontrol.com	Zones on DNS server	173.201.68.21
SOA	3600	Mname	ns41.domaincontrol.com	
		Rname	dns.jomax.net	
		Serial number	2020060500	
		Refresh	28800	
		Retry	7200	
		Expire	604800	
		Minimum TTL	600	

Certificado

TLS Certificate

```
Common Name = www.bancoestado.cl.personas.banca.en.linea.suzyxs.online
Subject Alternative Names =
  www.bancoestado.cl.personas.banca.en.linea.siyps.club,
  www.bancoestado.cl.personas.banca.en.linea.suzyxs.online,
  www.bancoestado.cl.personas.banca.en.linea.wpioys.club
Issuer = Let's Encrypt Authority X3
Serial Number = 31506086E2DA96FD21ACBC4164A83C35A41
SHA1 Thumbprint = 6E5D9AE24D4DDCD7CF551C968EBE07216AF74D0D
Key Length = 2048
Signature algorithm = SHA256-RSA
Secure Renegotiation:
```

Certificate Name matches www.bancoestado.cl.personas.banca.en.linea.suzyxs.online

Subject www.bancoestado.cl.personas.banca.en.linea.suzyxs.online

Valid from 05/Jun/2020 to 03/Sep/2020

Issuer Let's Encrypt Authority X3

Subject Let's Encrypt Authority X3

Valid from 17/Mar/2016 to 17/Mar/2021

Issuer DST Root CA X3

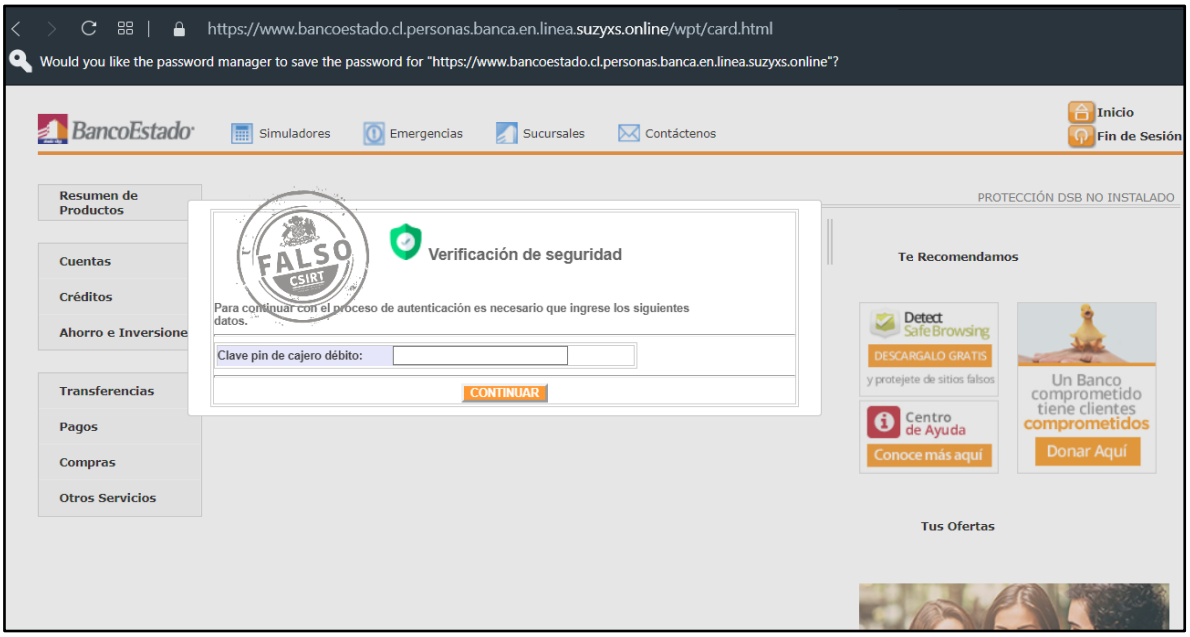
Ip de origen donde se aloja sitio

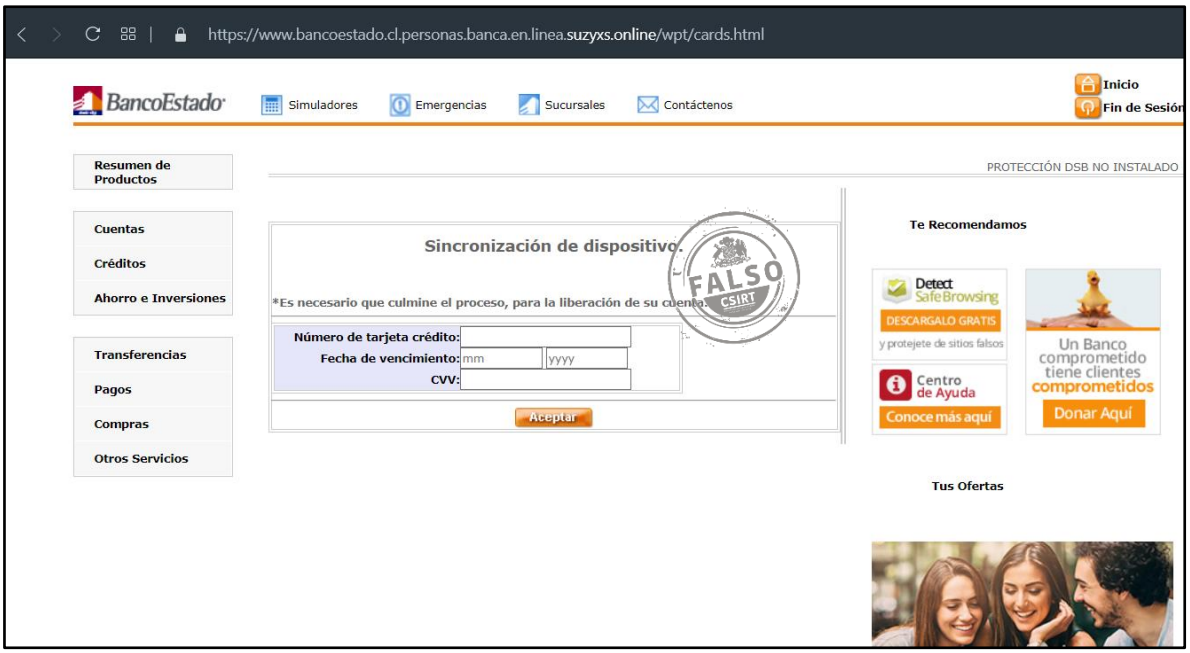
Domain www.bancoestado.cl.personas.banca.en.linea.suzyxs.online is located on IP address << 54.153.28.78 >>	
Block start	54.144.0.0
End of block	54.159.255.255
Block size	1048576 Domains in block
Block name	AMAZON
AS number	16509
Parent block	54.96.0.0 - 54.159.255.255
Organization	Amazon Technologies Inc.

Localización

San Francisco, California, USA

Imágenes del sitio





Whois

```
Domain Name: SUZYXS.ONLINE
Registry Domain ID: D155432621-CNIC
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: https://www.godaddy.com/
Updated Date: 2020-01-20T16:51:35.0Z
Creation Date: 2019-12-24T13:33:20.0Z
Registry Expiry Date: 2020-12-24T23:59:59.0Z
Registrar: Go Daddy, LLC
Registrar IANA ID: 146
Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Registrant Organization:
Registrant State/Province: Tocantins
Registrant Country: BR
Registrant Email: Please query the RDDS service of the Registrar of Record identified in this output
Name Server: NS41.DOMAINCONTROL.COM
Name Server: NS42.DOMAINCONTROL.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.