Alerta de seguridad informática	8FFR20-00207-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	05 de febrero de 2020
Última revisión	05 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 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

bancaestado[.]sytes[.]net

Domain bancaestado.sytes.net

bancaestado / sytes / net / Subdomains

record type	TTL	value
A	60	45.155.37.107

Domain sytes.net

sytes / net / Subdomains

record type	TTL	value		
A	60	8.23.224.108		
NS	86400	nf1.no-ip.com	Zones on DNS server	194.62.182.53
NS	86400	nf2.no-ip.com	Zones on DNS server	45.54.64.53
NS	86400	nf3.no-ip.com	Zones on DNS server	204.16.253.53
NS	86400	nf4.no-ip.com	Zones on DNS server	194.62.183.53
NS	86400	nf5.no-ip.com	Zones on DNS server	204.16.253.53
MX	600	10 mail2.no-ip.com		69.65.5.119
TXT	360	v=spf1 include:no-ip.com -all		
SOA	60	Mname	nf1.no-ip.com	
		Rname	hostmaster.no-ip.com	
		Serial number	2086508016	
		Refresh	600	
		Retry	300	
		Expire	604800	
		Minimum TTL	600	

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

Certificados

Subject DN CN=bancaestado.sytes.net

Issuer DN C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3

Serial 305214286629010055472298085857914855734412

Validity 2020-02-04 17:33:38 **to** 2020-05-04 17:33:38 (90 days, 0:00:00)

Names bancaestado.sytes.net

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

IP

45[.]155[.]37[.]107

Domain bancaestado.sytes.net is located on IP address << 45.155.37.107 >>

Block start	45.155.36.0
End of block	45.155.39.255
Block size	1024 Domains in block
Block name	US-SHOCK11-20190917
AS number	395092
Parent block	45.128.0.0 - 45.159.255.255
Organization	ORG-SHL36-RIPE
City	Amsterdam
Region/State	Noord-Holland
Country	NL , Netherlands
Reg. date	2019-09-17
Host name	no record in reverse zone

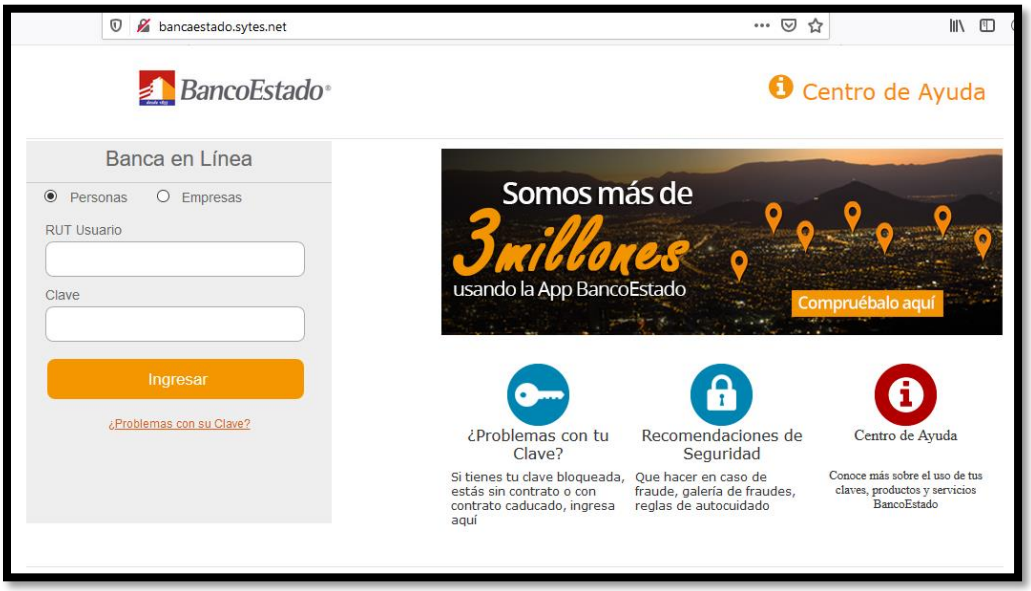
Ilustración 3 Ip de Origen donde se aloja Sitio Falso del Banco Estado.

Localización

Edinburgh, Scotland

Location	Maidenhead, England, United Kingdom (GB)
Latitude and Longitude	51.5, -0.69

Imagen del sitio



Whois

```
Domain Name: sytes.net
Registry Domain ID: 5534045_DOMAIN_NET-VRSN
Registrar WHOIS Server: whois.srsplus.com
Registrar URL: http://srsplus.com
Updated Date: 2017-01-31T17:05:30Z
Creation Date: 1999-04-22T04:00:00Z
Registrar Registration Expiration Date: 2021-04-22T04:00:00Z
Registrar: TLDS LLC. d/b/a SRSPlus
Registrar IANA ID: 320
Reseller:
Domain Status: clientTransferProhibited http://icann.org/epp#clientTransferProhibited
Registry Registrant ID:
Registrant Name: Dan Durrer
Registrant Organization: No-IP.com
Registrant Street: 425 Maestro  Dr. Second Floor
Registrant City: Reno
Registrant State/Province: NV
Registrant Postal Code: 89511
Registrant Country: US
Registrant Phone: +1.7758531883
Registrant Phone Ext.:
Registrant Fax:
Registrant Fax Ext.:
Registrant Email: domains@no-ip.com
Registry Admin ID:
Admin Name: Dan Durrer
Admin Organization: No-IP.com
Admin Street: 425 Maestro  Dr. Second Floor
Admin City: Reno
Admin State/Province: NV
Admin Postal Code: 89511
Admin Country: US
Admin Phone: +1.7758531883
Admin Phone Ext.:
Admin Fax:
Admin Fax Ext.:
Admin Email: domains@no-ip.com
Registry Tech ID:
Tech Name: Dan Durrer
Tech Organization: No-IP.com
Tech Street: 425 Maestro  Dr. Second Floor
Tech City: Reno
Tech State/Province: NV
Tech Postal Code: 89511
Tech Country: US
Tech Phone: +1.7758531883
Tech Phone Ext.:
Tech Fax:
Tech Fax Ext.:
Tech Email: domains@no-ip.com
Name Server: nf3.no-ip.com
Name Server: nf2.no-ip.com
Name Server: nf4.no-ip.com
Name Server: nf1.no-ip.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: 2020.02.05 10:07:29 -03'00'