Alerta de seguridad informática	8FFR20-00253-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	11 de Marzo de 2020
Última revisión	11 de Marzo 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 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

URL´s

empresasbancestado[.]hopto[.]org

Domain empresasbancestado.hopto.org

empresasbancestado / hopto / org / Subdomains

record type	TTL	value
A	60	45.155.37.115

Domain hopto.org

hopto / org / 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	1800	5 mail1.no-ip.com		
MX	1800	10 mail2.no-ip.com		69.65.5.119
SOA	60	Mname	nf1.no-ip.com	
		Rname	hostmaster.no-ip.com	
		Serial number	2058256516	
		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=empresasbancestado.hopto.org
Issuer DN	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
Serial	384887168814485071891200563146720766826691
Validity	2020-03-09 19:34:29 to 2020-06-07 19:34:29 (90 days, 0:00:00)
Names	empresasbancestado.hopto.org

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

IP
45[.]155[.]37[.]115

Domain empresasbancestado.hopto.org is located on IP address << 45.155.37.115 >>

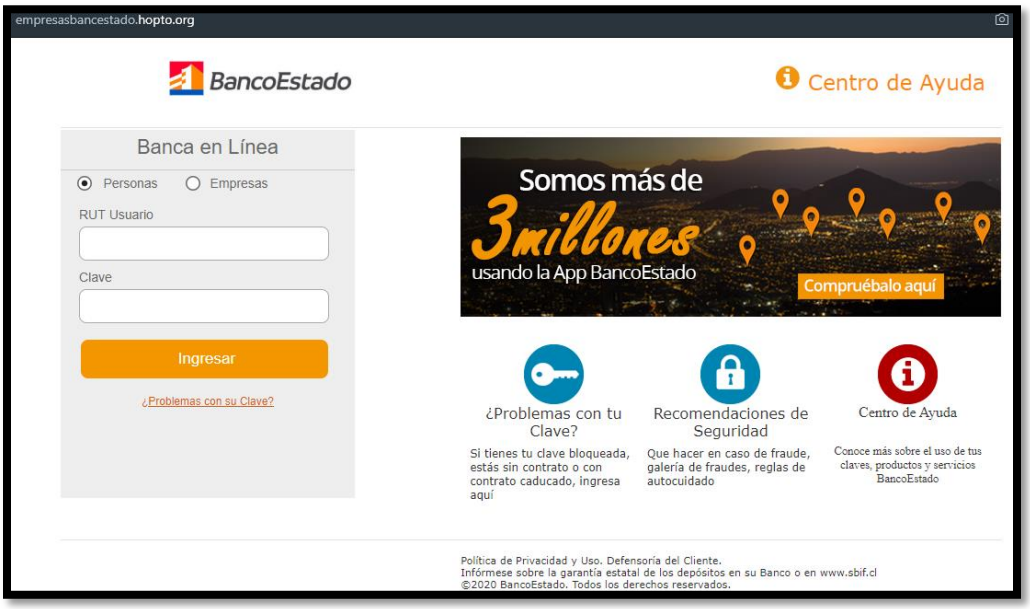
Block start	45.155.36.0
End of block	45.155.39.255
Block size	1024 Domains in block
Block name	US-SHOCK11-20190917
AS number	395092
Parent block	45.128.0.0 - 45.159.255.255
Organization	ORG-SHL36-RIPE

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

Localización
Reino Unido

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

Imagen del sitio



Whois

```
Domain Name: HOPTO.ORG
Registry Domain ID: D20065021-LROR
Registrar WHOIS Server: whois.networksolutions.com
Registrar URL: http://www.srsplus.com
Updated Date: 2017-01-31T17:05:12Z
Creation Date: 2000-02-17T19:56:50Z
Registry Expiry Date: 2021-02-17T19:56:50Z
Registrar Registration Expiration Date:
Registrar: TLDS L.L.C. d/b/a SRSPlus
Registrar IANA ID: 320
Registrar Abuse Contact Email: abuse@web.com
Registrar Abuse Contact Phone: +1.8003337680
Reseller:
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Registrant Organization: No-IP.com
Registrant State/Province: NV
Registrant Country: US
Name Server: NF1.NO-IP.COM
Name Server: NF2.NO-IP.COM
Name Server: NF3.NO-IP.COM
Name Server: NF4.NO-IP.COM
Name Server: NF5.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: 2020.03.10 22:51:54 -03'00'