Alerta de seguridad informática	8FFR20-00259-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	12 de Marzo de 2020
Última revisión	12 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

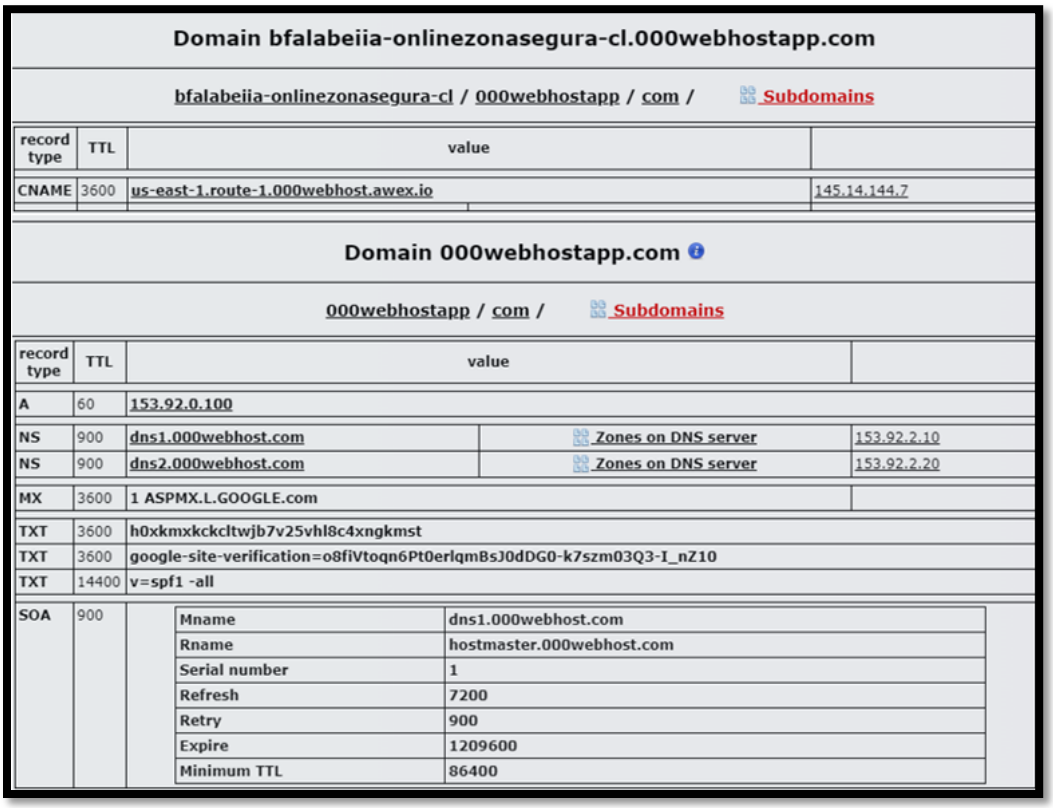
El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de un portal fraudulento asociado a una IP que suplanta el sitio web oficial del **Banco Falabella**, el que podría servir para robar credenciales de usuarios de esa entidad.

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

bfalabeiia-onlinezonasegura-cl[.]000webhostapp[.]com



Domain bfalabeiia-onlinezonasegura-cl.000webhostapp.com

bfalabeiia-onlinezonasegura-cl / 000webhostapp / com / Subdomains

record type	TTL	value	
CNAME	3600	us-east-1.route-1.000webhost.awex.io	145.14.144.7

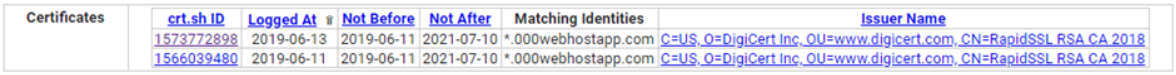
Domain 000webhostapp.com

000webhostapp / com / Subdomains

record type	TTL	value		
A	60	153.92.0.100		
NS	900	dns1.000webhost.com	Zones on DNS server	153.92.2.10
NS	900	dns2.000webhost.com	Zones on DNS server	153.92.2.20
MX	3600	1 ASPMX.L.GOOGLE.com		
TXT	3600	h0xkmxkckcltwjb7v25vhl8c4xngkmst		
TXT	3600	google-site-verification=o8fiVtoqn6Pt0erlqmBsJ0dDG0-k7szm03Q3-I_nZ10		
TXT	14400	v=spf1 -all		
SOA	900	Mname: dns1.000webhost.com Rname: hostmaster.000webhost.com Serial number: 1 Refresh: 7200 Retry: 900 Expire: 1209600 Minimum TTL: 86400		

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

Certificados



Certificates

crt.sh ID	Logged At	Not Before	Not After	Matching Identities	Issuer Name
1573772898	2019-06-13	2019-06-11	2021-07-10	*.000webhostapp.com	C=US, O=DigiCert Inc, OU=www.digicert.com, CN=RapidSSL RSA CA 2018
1566039480	2019-06-11	2019-06-11	2021-07-10	*.000webhostapp.com	C=US, O=DigiCert Inc, OU=www.digicert.com, CN=RapidSSL RSA CA 2018

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

IP
145[.]14[.]145[.]168

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

Localización
Estados Unidos

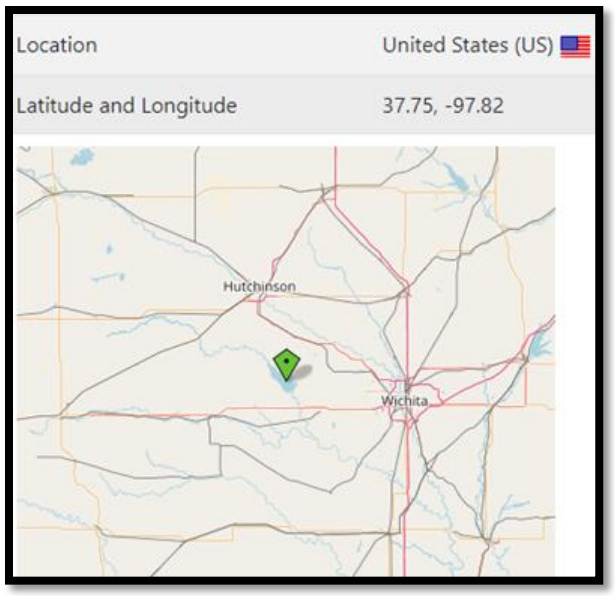


Imagen del sitio

Whois

```
Domain Name: 000WEBHOSTAPP.COM
Registry Domain ID: 2027404438_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.hostinger.com
Registrar URL: https://www.hostinger.com
Updated Date: 2017-04-05T08:09:44Z
Creation Date: 2016-05-11T13:34:12Z
Registrar Registration Expiration Date: 2022-05-11T13:34:12Z
Registrar: Hostinger, UAB
Registrar IANA ID: 1636
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProh
ibited
Registry Registrant ID: GDPR Masked
Registrant Name: GDPR Masked
Registrant Organization: GDPR Masked
Registrant Street: GDPR Masked
Registrant City: GDPR Masked
Registrant State/Province: Larnaka
Registrant Postal Code: GDPR Masked
Registrant Country: CY
Registrant Phone: GDPR Masked
Registrant Phone Ext:
Registrant Fax: GDPR Masked
Registrant Fax Ext:
Registrant Email: gdpr-masking@gdpr-masked.com
Registry Admin ID: GDPR Masked
Admin Name: GDPR Masked
Admin Organization: GDPR Masked
Admin Street: GDPR Masked
Admin City: GDPR Masked
Admin State/Province: GDPR Masked
Admin Postal Code: GDPR Masked
Admin Country: GDPR Masked
Admin Phone: GDPR Masked
Admin Phone Ext:
Admin Fax: GDPR Masked
Admin Fax Ext:
Admin Email: gdpr-masking@gdpr-masked.com
Registry Tech ID: GDPR Masked
Tech Name: GDPR Masked
Tech Organization: GDPR Masked
Tech Street: GDPR Masked
Tech City: GDPR Masked
Tech State/Province: GDPR Masked
Tech Postal Code: GDPR Masked
Tech Country: GDPR Masked
Tech Phone: GDPR Masked
Tech Phone Ext:
Tech Fax: GDPR Masked
Tech Fax Ext:
Tech Email: gdpr-masking@gdpr-masked.com
Name Server: dns1.000webhost.com
Name Server: dns2.000webhost.com
DNSSEC: Unsigned
Registrar Abuse Contact Email: abuse@hostinger.com
Registrar Abuse Contact Phone: +37064503378
```

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: 2020.03.12 11:25:21 -03'00'