Alerta de seguridad informática	8FFR20-00197-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	28 de Enero de 2020
Última revisión	28 de Enero 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 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

URL Sitio Clonado:
birdseye-security[.]com/www[.]bancoestado[.]cl/imagenes/comun2008/banca-en-linea-personas[.]htm

URL Re-direccionador:

bit[.]ly/BancoEstado_activacion

Domain birdseye-security.com

birdseye-security / com / Subdomains

record type	TTL	value		
A	1200	63.250.36.8		
NS	86400	ns2.marque-hosting.com	Zones on DNS server	63.250.36.8
NS	86400	ns1.marque-hosting.com	Zones on DNS server	63.250.36.8
MX	1200	0 mail.birdseye-security.com		
SOA	86400	Mname: ns1.marque-hosting.com Rname: camf16.live.com Serial number: 2020012505 Refresh: 3600 Retry: 1800 Expire: 1209600 Minimum TTL: 86400		

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

Certificados

Subject DN CN=birdseye-security.com

Issuer DN C=US, ST=TX, L=Houston, O=cPanel, Inc., CN=cPanel, Inc. Certification Authority

Serial 332644953794482429353128715316408734569

Validity 2019-12-22 00:00:00 **to** 2020-03-21 23:59:59 (90 days, 23:59:59)

Names birdseye-security.com
cpanel.birdseye-security.com
mail.birdseye-security.com
webdisk.birdseye-security.com
webmail.birdseye-security.com
www.birdseye-security.com

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

IP

63.250.36.8

Domain birdseye-security.com is located on IP address << 63.250.36.8 >>	
Block start	63.250.36.0
End of block	63.250.37.255
Block size	512 Domains in block
Block name	NAQUE3623
AS number	22612
Parent block	63.250.0.0 - 63.250.63.255
Organization	Nague IT
City	Atlanta
Region/State	Georgia
Country	US , United States
Reg. date	2011-09-20
Host name	consulting-creditor.quarantine-pnap.web-hosting.com

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

Localización

Atlanta, Georgia, Estados Unidos

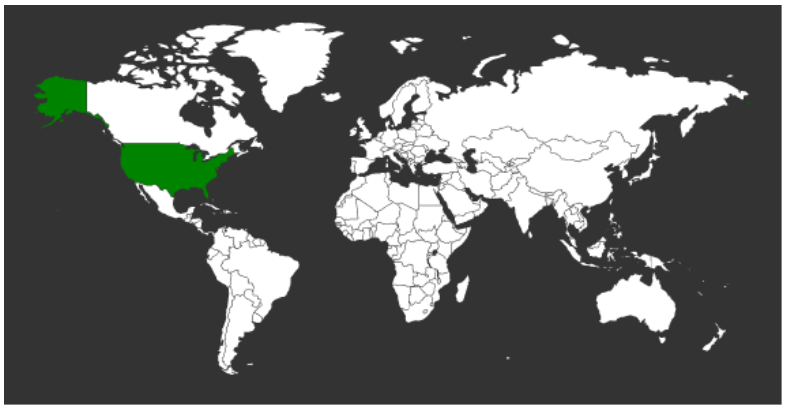
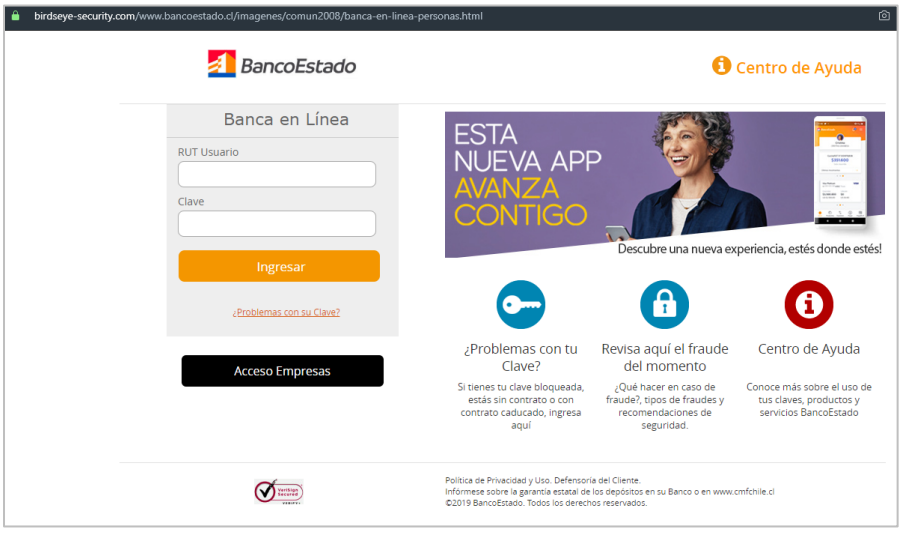


Imagen del sitio



Whois

```
Domain name: birdseye-security.com
Registry Domain ID: 2334006438_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.namecheap.com
Registrar URL: http://www.namecheap.com
Updated Date: 2019-10-30T20:27:49.05Z
Creation Date: 2018-11-18T19:04:32.00Z
Registrar Registration Expiration Date: 2020-11-18T19:04:32.00Z
Registrar: NAMECHEAP INC
Registrar IANA ID: 1068
Registrar Abuse Contact Email: abuse@namecheap.com
Registrar Abuse Contact Phone: +1.6613102107
Reseller: NAMECHEAP INC
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Registry Registrant ID:
Registrant Name: WhoisGuard Protected
Registrant Organization: WhoisGuard, Inc.
Registrant Street: P.O. Box 0823-03411
Registrant City: Panama
Registrant State/Province: Panama
Registrant Postal Code:
Registrant Country: PA
Registrant Phone: +507.8365503
Registrant Phone Ext:
Registrant Fax: +51.17057182
Registrant Fax Ext:
Registrant Email: 3ed1f2245bed4d53bdd7e50255366ba3.protect@whoisguard.com
Registry Admin ID:
Admin Name: WhoisGuard Protected
Admin Organization: WhoisGuard, Inc.
Admin Street: P.O. Box 0823-03411
Admin City: Panama
Admin State/Province: Panama
Admin Postal Code:
Admin Country: PA
Admin Phone: +507.8365503
Admin Phone Ext:
Admin Fax: +51.17057182
Admin Fax Ext:
Admin Email: 3ed1f2245bed4d53bdd7e50255366ba3.protect@whoisguard.com
Registry Tech ID:
Tech Name: WhoisGuard Protected
Tech Organization: WhoisGuard, Inc.
Tech Street: P.O. Box 0823-03411
Tech City: Panama
Tech State/Province: Panama
Tech Postal Code:
Tech Country: PA
Tech Phone: +507.8365503
Tech Phone Ext:
Tech Fax: +51.17057182
Tech Fax Ext:
Tech Email: 3ed1f2245bed4d53bdd7e50255366ba3.protect@whoisguard.com
Name Server: ns1.marque-hosting.com
Name Server: ns2.marque-hosting.com
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2020-01-27T03:28:03.59Z <<<
```

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.