Alerta de seguridad informática	8FFR20-00204-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	04 de Febrero de 2020
Última revisión	04 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

URLs

banco[.]estadomovil[.]cl[.]autoatencionpizza[.]cl/profesional/imagenes/comun2008/banca-en-linea-personas[.]html
cbtservicesfl[.]com/iou7/imagenes/comun2008/banca-en-linea-personas[.]html
wokecogent[.]com/www[.]bancoestado[.]cl/imagenes/comun2008/banca-en-linea-personas[.]html

Domain autoatencionpizza.cl

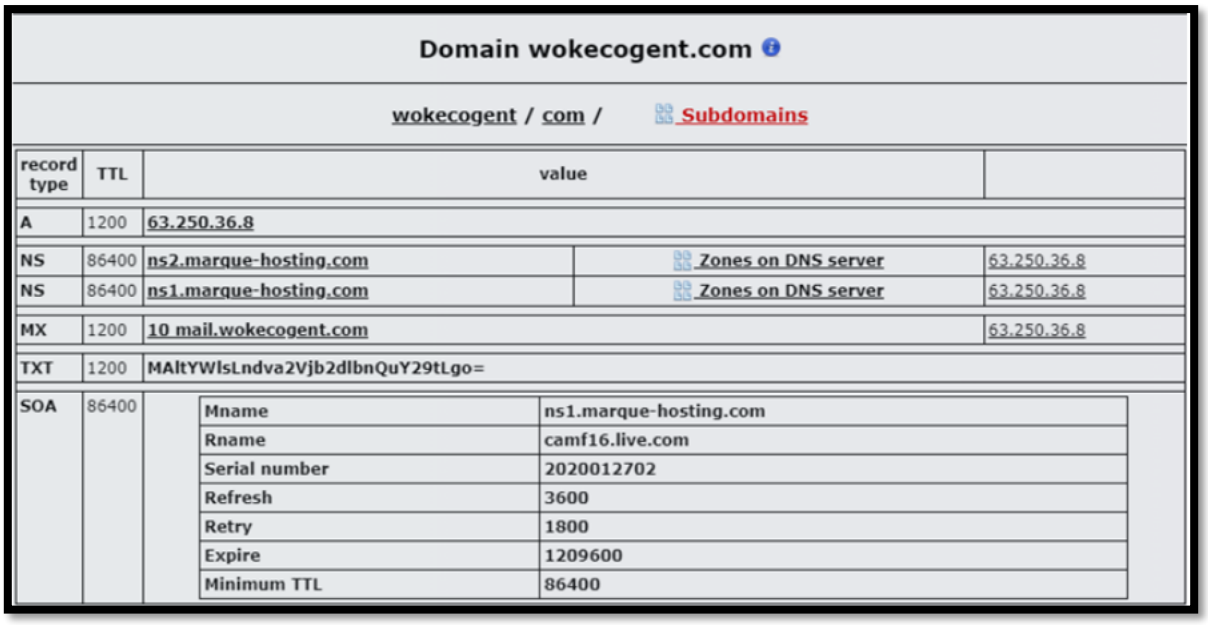
autoatencionpizza / cl / Subdomains

record type	TTL	value		
A	14400	54.39.37.193		
NS	86400	ns21.v2net.cl	Zones on DNS server	54.39.37.193
NS	86400	ns22.v2net.cl	Zones on DNS server	54.39.37.193
MX	14400	0 autoatencionpizza.cl		
TXT	14400	v=spf1 +a +mx +ip4:54.39.37.193 ~all		
SOA	86400	Mname	ns21.v2net.cl	
		Rname	mcontrerasv2.gmail.com	
		Serial number	2020020214	
		Refresh	3600	
		Retry	1800	
		Expire	1209600	
		Minimum TTL	86400	

Domain cbtservicesfl.com

cbtservicesfl / com / Subdomains

record type	TTL	value		
A	10800	107.180.3.140		
NS	3600	ns11.domaincontrol.com	Zones on DNS server	97.74.105.6
NS	3600	ns12.domaincontrol.com	Zones on DNS server	173.201.73.6
MX	3600	0 cbtservicesfl-com.mail.protection.outlook.com		
TXT	3600	v=spf1 include:spf.protection.outlook.com -all		
SOA	600	Mname	ns11.domaincontrol.com	
		Rname	dns.jomax.net	
		Serial number	2018052001	
		Refresh	28800	
		Retry	7200	
		Expire	604800	
		Minimum TTL	600	



Domain wokecogent.com

wokecogent / 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	10 mail.wokecogent.com		63.250.36.8
TXT	1200	MAltYWlsLndva2Vjb2dlbnQuY29tLgo=		
SOA	86400			

Mname	ns1.marque-hosting.com
Rname	camf16.live.com
Serial number	2020012702
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=banco.estadomovil.cl.autoatencionpizza.cl
Issuer DN	C=US, ST=TX, L=Houston, O=cPanel, Inc., CN=cPanel, Inc. Certification Authority
Serial	307301952596830838542774129062549209881
Validity	2020-02-02 00:00:00 **to** 2020-05-02 23:59:59 (90 days, 23:59:59)
Names	banco.estadomovil.cl.autoatencionpizza.cl www.banco.estadomovil.cl.autoatencionpizza.cl

Criteria	Type: Identity Match: ILIKE Search: 'cbtservicesfl.com'
Certificates	*None found*

Subject DN	C=US, ST=CA, L=San Francisco, O=CloudFlare, Inc., CN=sni.cloudflaressl.com
Issuer DN	C=US, ST=CA, L=San Francisco, O=CloudFlare, Inc., CN=CloudFlare Inc ECC CA-2
Serial	183119726778731860283851541473568221 8
Validity	2019-06-06 00:00:00 **to** 2020-06-05 12:00:00 (365 days, 12:00:00)
Names	*.wokecogent.com sni.cloudflaressl.com wokecogent.com

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

IPs

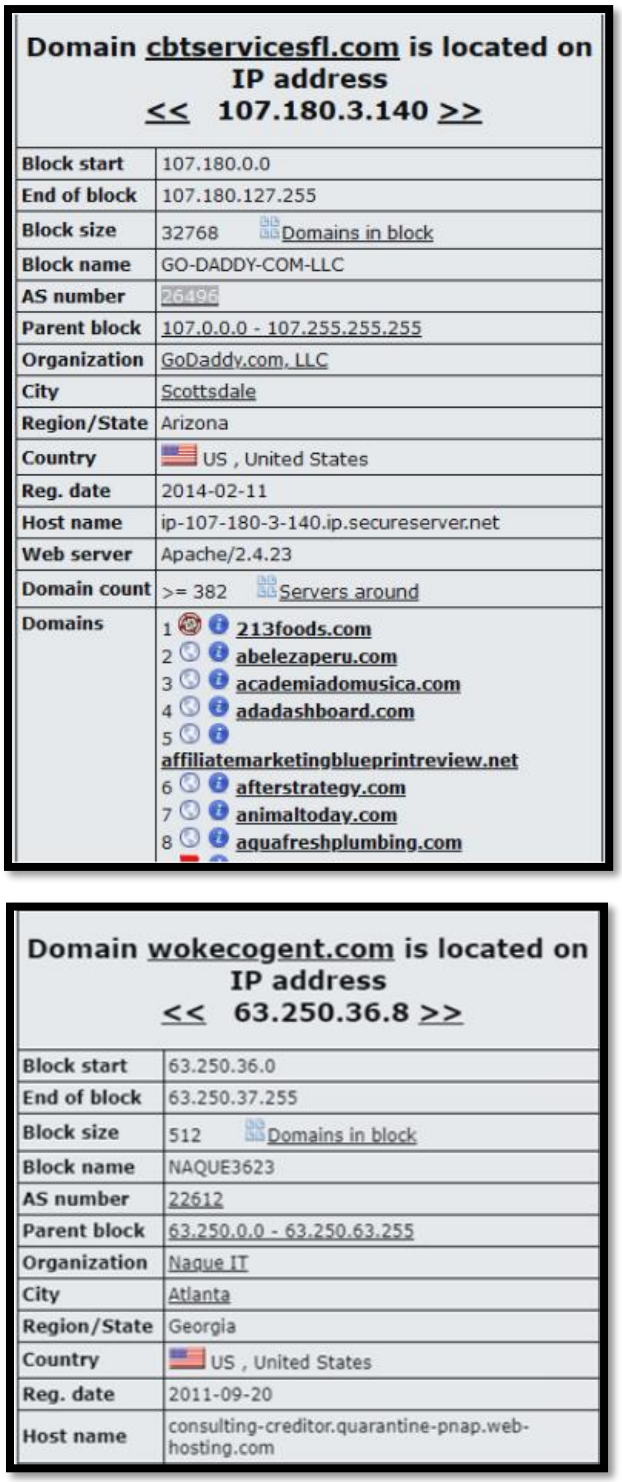
54[.]39[.]37[.]193

107[.]180[.]3[.]140

63[.]250[.]36[.]8

Domain banco.estadomovil.cl.autoatencionpizza.cl is located on IP address << 54.39.37.193 >>

Block start	54.0.0.0
End of block	54.63.255.255
Block size	4194304 Domains in block
Block name	MERCK2
AS number	16276
Parent block	54.0.0.0 - 54.255.255.255
Organization	Merck and Co., Inc.
City	Rahway
Region/State	New Jersey
Country	US , United States 40735
Reg. date	1992-03-17
Host name	morty.v2net.cl
Domain count	>= 3 Servers around
Domains	1 **2019miservicios.com** 2 **banco.estadomovil.cl.autoatencionpizza.cl** 3 **www.informaciondepi.com**



Domain cbtservicesfl.com is located on IP address << 107.180.3.140 >>	
Block start	107.180.0.0
End of block	107.180.127.255
Block size	32768 Domains in block
Block name	GO-DADDY-COM-LLC
AS number	26496
Parent block	107.0.0.0 - 107.255.255.255
Organization	GoDaddy.com, LLC
City	Scottsdale
Region/State	Arizona
Country	US , United States
Reg. date	2014-02-11
Host name	ip-107-180-3-140.ip.secureserver.net
Web server	Apache/2.4.23
Domain count	>= 382 Servers around
Domains	1 213foods.com 2 abelezaperu.com 3 academiadomusica.com 4 adadashboard.com 5 affiliatemarketingblueprintreview.net 6 afterstrategy.com 7 animaltoday.com 8 aquafreshplumbing.com

Domain wokecogent.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

Canadá Montreal, Quebec

USA, Scottsdale, Arizona

USA, Atlanta, Georgia

Location	Los Angeles, California, United States (US)
Latitude and Longitude	34.03, -118.43

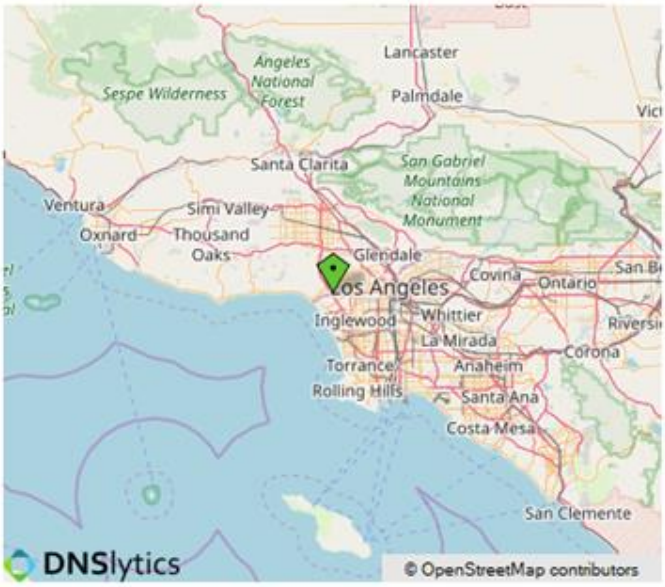
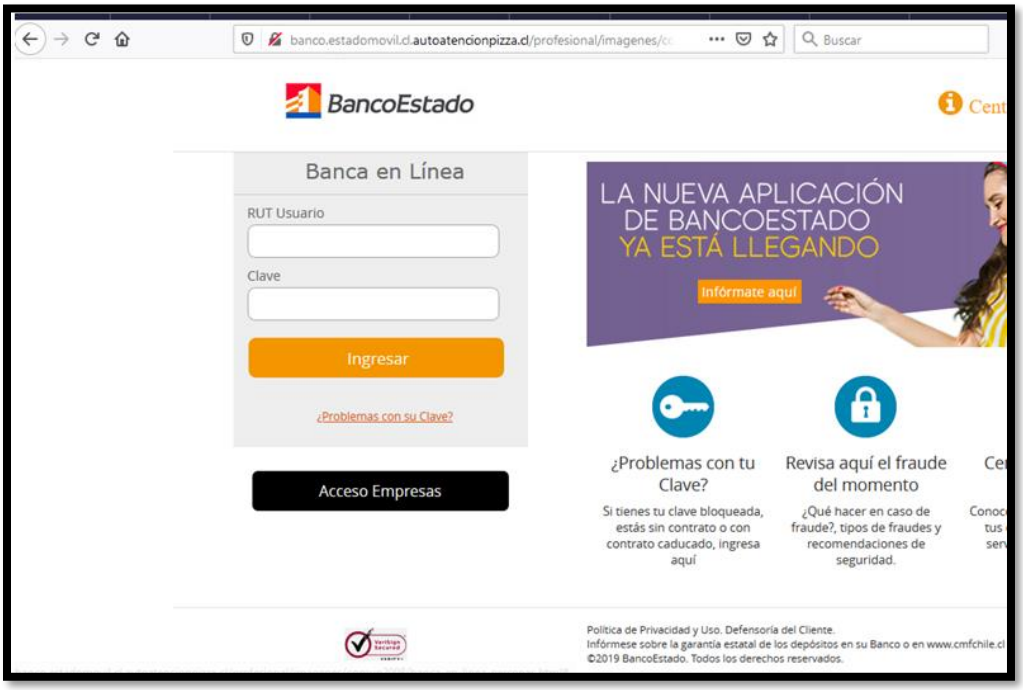
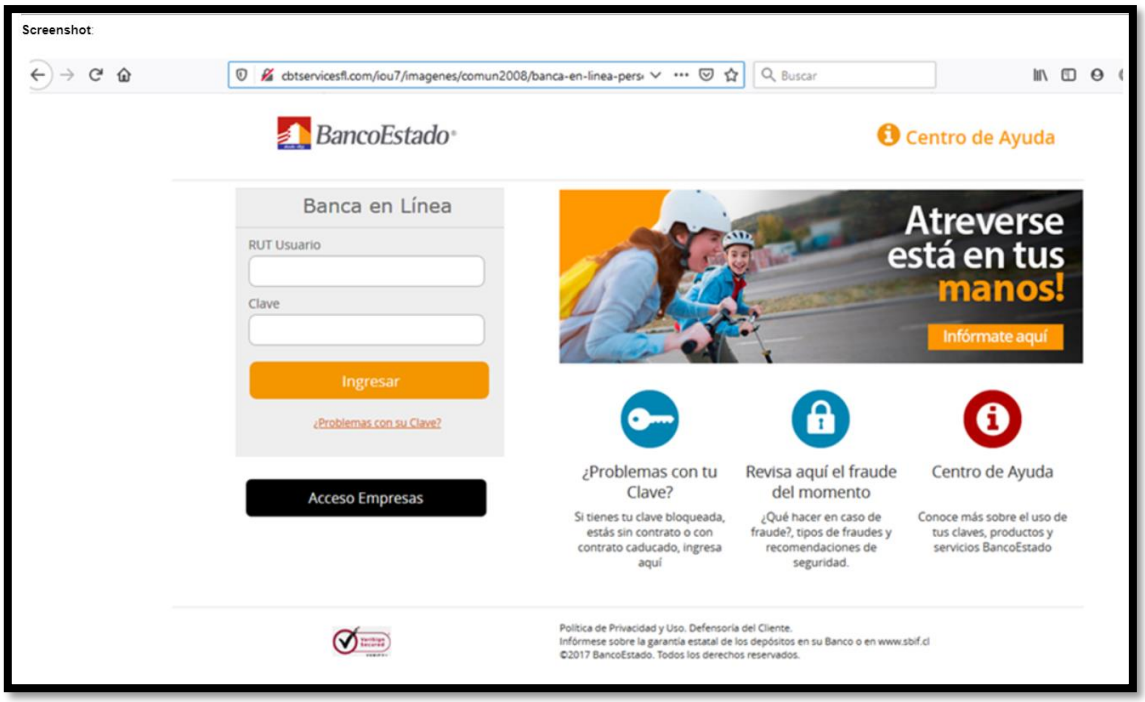
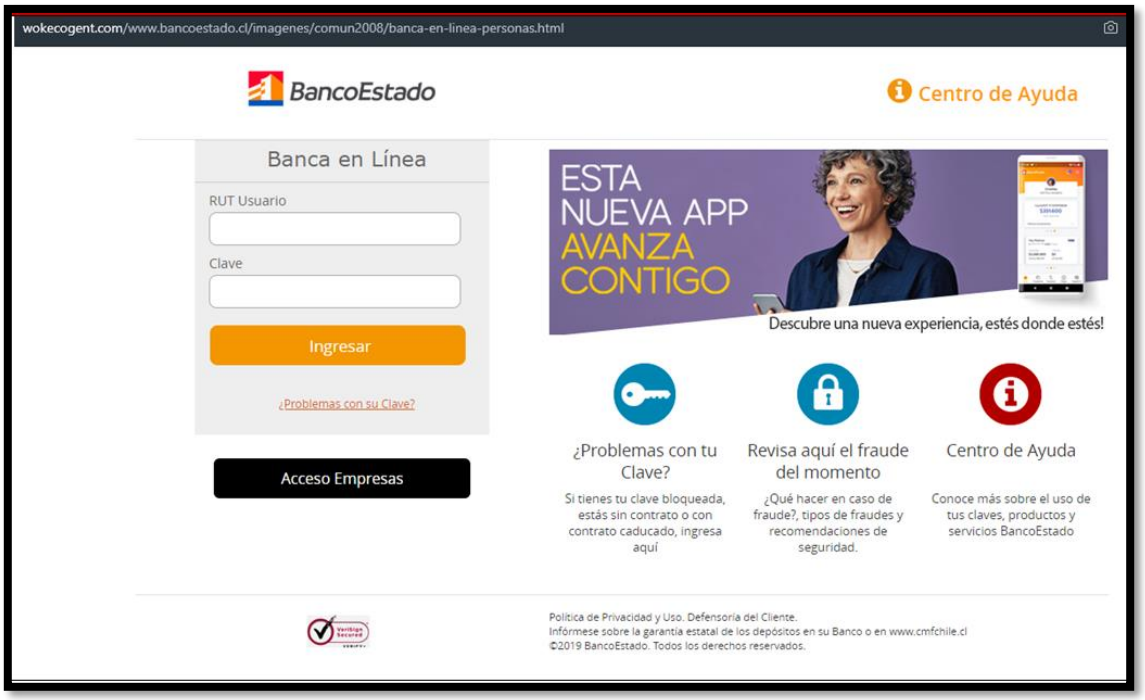


Imagen del sitio




Screenshot:
cbtservicesfl.com/iou7/imagenes/comun2008/banca-en-linea-pers
Buscar
BancoEstado
Centro de Ayuda
Banca en Línea
RUT Usuario
Clave
Ingresar
¿Problemas con su Clave?
Acceso Empresas
Atreverse está en tus manos!
Infórmate aquí
¿Problemas con tu Clave?
Si tienes tu clave bloqueada, estás sin contrato o con contrato caducado, ingresa aquí
Revisa aquí el fraude del momento
¿Qué hacer en caso de fraude?, tipos de fraudes y recomendaciones de seguridad.
Centro de Ayuda
Conoce más sobre el uso de tus claves, productos y servicios BancoEstado
Política de Privacidad y Uso. Defensoría del Cliente.
Infórmese sobre la garantía estatal de los depósitos en su Banco o en www.sbif.cl
©2017 BancoEstado. Todos los derechos reservados.


wokecogent.com/www.bancoestado.cl/imagenes/comun2008/banca-en-linea-personas.html
BancoEstado
Centro de Ayuda
Banca en Línea
RUT Usuario
Clave
Ingresar
¿Problemas con su Clave?
Acceso Empresas
ESTA NUEVA APP AVANZA CONTIGO
Descubre una nueva experiencia, estés donde estés!
¿Problemas con tu Clave?
Si tienes tu clave bloqueada, estás sin contrato o con contrato caducado, ingresa aquí
Revisa aquí el fraude del momento
¿Qué hacer en caso de fraude?, tipos de fraudes y recomendaciones de seguridad.
Centro de Ayuda
Conoce más sobre el uso de tus claves, productos y servicios BancoEstado
Política de Privacidad y Uso. Defensoría del Cliente.
Infórmese sobre la garantía estatal de los depósitos en su Banco o en www.cmfchile.cl
©2019 BancoEstado. Todos los derechos reservados.

Whois

```
soc@ITQ-ivps2:~$ whois autoatencionpizza.cl
%%
%% This is the NIC Chile Whois server (whois.nic.cl).
%%
%% Rights restricted by copyright.
%% See https://www.nic.cl/normativa/politica-publicacion-de-datos-cl.pdf
%%

Domain name: autoatencionpizza.cl
Registrant name: Jose Rosas
Registrant organisation: AutoAtencion Pizza
Registrar name: Hosting Concepts B.V. d/b/a Registrar.eu
Registrar URL: https://www.openprovider.es
Creation date: 2019-12-13 00:19:39 CLST
Expiration date: 2020-12-13 00:19:39 CLST
Name server: ns21.v2net.cl
Name server: ns22.v2net.cl
```

```
Domain Name: cbtservicesfl.com
Registry Domain ID: 2098352404_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: http://www.godaddy.com
Updated Date: 2017-02-17T03:09:20Z
Creation Date: 2017-02-17T03:09:20Z
Registrar Registration Expiration Date: 2020-02-17T03:09:20Z
Registrar: GoDaddy.com, LLC
Registrar IANA ID: 146
Registrar Abuse Contact Email: abuse@godaddy.com
Registrar Abuse Contact Phone: +1.4806242505
Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited http://www.icann.org/epp#clientUpdateProhibited
Domain Status: clientRenewProhibited http://www.icann.org/epp#clientRenewProhibited
Domain Status: clientDeleteProhibited http://www.icann.org/epp#clientDeleteProhibited
Registry Registrant ID: Not Available From Registry
Registrant Name: Registration Private
Registrant Organization: Domains By Proxy, LLC
Registrant Street: DomainsByProxy.com
Registrant Street: 14455 N. Hayden Road
Registrant City: Scottsdale
Registrant State/Province: Arizona
Registrant Postal Code: 85260
Registrant Country: US
Registrant Phone: +1.4806242599
Registrant Phone Ext:
Registrant Fax: +1.4806242598
Registrant Fax Ext:
Registrant Email: cbtservicesfl.com@domainsbyproxy.com
Registry Admin ID: Not Available From Registry
Admin Name: Registration Private
Admin Organization: Domains By Proxy, LLC
Admin Street: DomainsByProxy.com
Admin Street: 14455 N. Hayden Road
Admin City: Scottsdale
Admin State/Province: Arizona
Admin Postal Code: 85260
Admin Country: US
Admin Phone: +1.4806242599
Admin Phone Ext:
Admin Fax: +1.4806242598
Admin Fax Ext:
```

```
Registrant Email: cbtservicesfl.com@domainsbyproxy.com
Registry Admin ID: Not Available From Registry
Admin Name: Registration Private
Admin Organization: Domains By Proxy, LLC
Admin Street: DomainsByProxy.com
Admin Street: 14455 N. Hayden Road
Admin City: Scottsdale
Admin State/Province: Arizona
Admin Postal Code: 85260
Admin Country: US
Admin Phone: +1.4806242599
Admin Phone Ext:
Admin Fax: +1.4806242598
Admin Fax Ext:
Admin Email: cbtservicesfl.com@domainsbyproxy.com
Registry Tech ID: Not Available From Registry
Tech Name: Registration Private
Tech Organization: Domains By Proxy, LLC
Tech Street: DomainsByProxy.com
Tech Street: 14455 N. Hayden Road
Tech City: Scottsdale
Tech State/Province: Arizona
Tech Postal Code: 85260
Tech Country: US
Tech Phone: +1.4806242599
Tech Phone Ext:
Tech Fax: +1.4806242598
Tech Fax Ext:
Tech Email: cbtservicesfl.com@domainsbyproxy.com
Name Server: NS11.DOMAINCONTROL.COM
Name Server: NS12.DOMAINCONTROL.COM
DNSSEC: unsigned
```

```
Domain Name: WOKECOGENT.COM
Registry Domain ID: 2399197096_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.namecheap.com
Registrar URL: http://www.namecheap.com
Updated Date: 2019-12-19T22:56:51Z
Creation Date: 2019-06-06T10:39:25Z
Registry Expiry Date: 2020-06-06T10:39:25Z
Registrar: NameCheap, Inc.
Registrar IANA ID: 1068
Registrar Abuse Contact Email: abuse@namecheap.com
Registrar Abuse Contact Phone: +1.6613102107
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Name Server: NS1.MARQUE-HOSTING.COM
Name Server: NS2.MARQUE-HOSTING.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: 2020.02.04 11:44:50 -03'00'