Alerta de seguridad informática	8FFR20-00182-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	15 de Enero de 2020
Última revisión	15 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 tres portales fraudulentos asociados a tres IPs que suplantan el sitio web oficial de Banco Estado, los que podrían 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:

18[.]231[.]168[.]68:85/www[.]banco[.]estado[.]cl[.]imagenies[.]comun2008[.]banca[.]enlinea[.]personas/index[.]html

foxflores[.]com[.]br/cmfchile/imagenes/comun2008/banca-en-linea-personas[.]html

sstawebm[.]com

IP address	18.231.168.68
Reverse DNS (PTR record)	ec2-18-231-168-68.sa-east-1.compute.amazonaws.com
DNS server (NS record)	x3.amazonaws.org (208.78.71.31) x1.amazonaws.com (156.154.64.10) x4.amazonaws.org (204.13.251.31) pdns1.ultradns.net (204.74.108.1) x2.amazonaws.com (156.154.65.10)

Domain foxflores.com.br

foxflores / com / br / Subdomains

record type	TTL	value		
A	86400	192.99.244.40		
NS	86400	ns1.foxflores.com.br	Zones on DNS server	192.99.244.40
NS	86400	ns2.foxflores.com.br	Zones on DNS server	192.99.244.40
MX	86400	10 mail.foxflores.com.br		192.99.244.40
TXT	86400	v=spf1 +a +mx +a:vps260891.battlecloud.club -all		
SOA	86400	Mname: ns2.foxflores.com.br Rname: office.battlecloud.club Serial number: 2019112202 Refresh: 10800 Retry: 3600 Expire: 604800 Minimum TTL: 10800		

Domain sstawebm.com

sstawebm / com / Subdomains

record type	TTL	value		
A	10800	107.180.48.66		
NS	3600	ns52.domaincontrol.com	Zones on DNS server	173.201.73.26
NS	3600	ns51.domaincontrol.com	Zones on DNS server	97.74.105.26
SOA	3600	Mname: ns51.domaincontrol.com Rname: dns.jomax.net Serial number: 2020011401 Refresh: 28800 Retry: 7200 Expire: 604800 Minimum TTL: 600		

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

Certificados

Subject DN CN=foxflores.com.br

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

Serial 288415281500201085715923453764279210492434

Validity 2019-11-22 09:23:06 **to** 2020-02-20 09:23:06 (90 days, 0:00:00)

Names *.foxflores.com.br
foxflores.com.br

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

IP

18.231.168.68
192.99.244.40
107.180.48.66

IP address << 18.231.168.68 >>

Block start	18.0.0.0
End of block	18.255.255.255
Block size	16777216 Domains in block
Block name	MIT
AS number	16509
Parent block	
Organization	MIT
City	Cambridge
Region/State	Massachusetts
Country	US , United States
Reg. date	1994-01-01
Host name	ec2-18-231-168-68.sa-east-1.compute.amazonaws.com
Domains	not found

Domain foxflores.com.br is located on IP address << 192.99.244.40 >>

Block start	192.99.0.0
End of block	192.99.255.255
Block size	65536 Domains in block
Block name	OVH-ARIN-7
AS number	16276
Parent block	192.0.0.0 - 192.255.255.255
Organization	OVH Hosting, Inc.
City	Montreal
Region/State	Quebec
Country	CA , Canada
Reg. date	2013-06-17
Host name	40.ip-192-99-244.net
Domains	1 foxflores.com.br

Domain sstawebm.com is located on IP address
<< 107.180.48.66 >>

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-107-180-48-66.ip.secureserver.net
Web server	Apache/2.4.23
Powered by	PHP/5.6.28

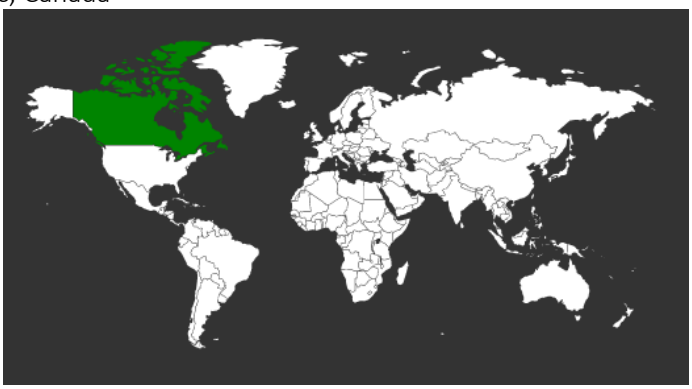
Ilustración 3 Ip de Origen donde se aloja Sitio Falso del Banco Estado

Localización
Sao Paulo, Brasil

Geo information

Location	São Paulo, Sao Paulo, Brazil (BR)
Latitude and Longitude	-23.57, -46.64

Beauharnois, Quebec, Canadá



Scottsdale, Arizona, Estados Unidos

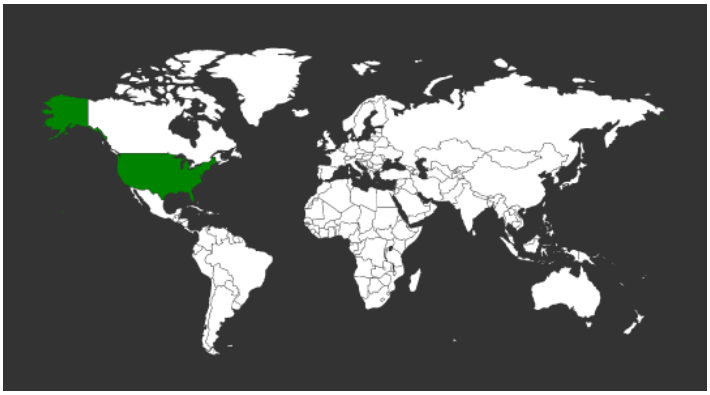
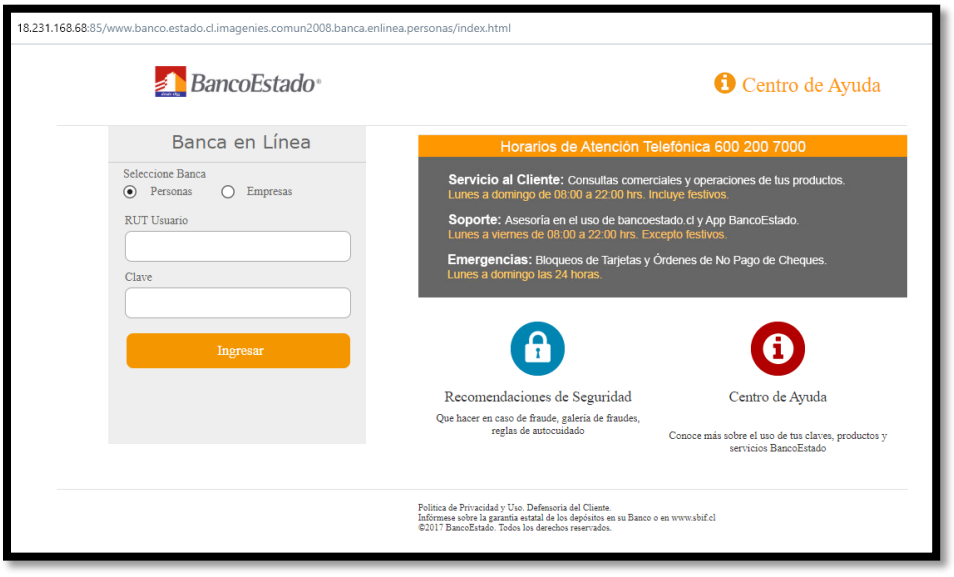
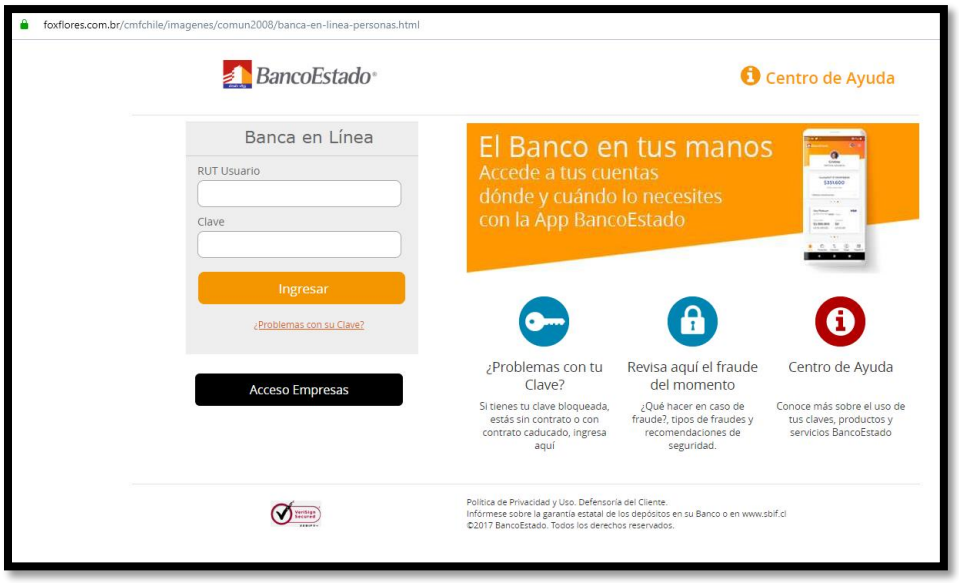
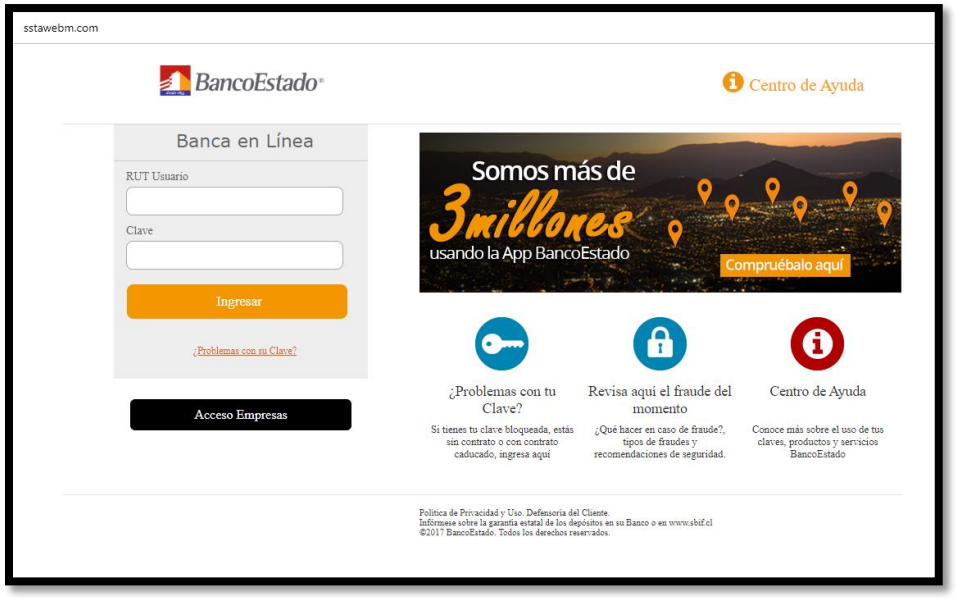


Imagen del sitio




foxflores.com.br/cmfchile/imagenes/comun2008/banca-en-linea-personas.html
BancoEstado
Centro de Ayuda
Banca en Línea
RUT Usuario
Clave
Ingresar
¿Problemas con su Clave?
Acceso Empresas
El Banco en tus manos
Accede a tus cuentas
dónde y cuándo lo necesites
con la App BancoEstado
¿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.


sstawebm.com
BancoEstado
Centro de Ayuda
Banca en Línea
RUT Usuario
Clave
Ingresar
¿Problemas con su Clave?
Acceso Empresas
Somos más de
3millones
usando la App BancoEstado
Compruébalo 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.

Whois

```
NetRange:       18.231.0.0 - 18.231.255.255
CIDR:           18.231.0.0/16
NetName:        AMAZON-GRU
NetHandle:      NET-18-231-0-0-2
Parent:         AT-88-Z (NET-18-128-0-0-1)
NetType:        Reallocated
OriginAS:       AS16509
Organization:   Amazon Data Services Brazil (ADSB-3)
RegDate:        2017-05-10
Updated:        2017-05-10
Ref:            https://rdap.arin.net/registry/ip/18.231.0.0


OrgName:        Amazon Data Services Brazil
OrgId:          ADSB-3
Address:        Complexo JK, Torre E
Address:        Avenida Presidente Juscelino Kubitschek, 2041, Itaim Bibi
City:           Sao Paulo
StateProv:      SP
PostalCode:     04543-011
Country:        BR
RegDate:        2015-12-09
Updated:        2019-08-02
Ref:            https://rdap.arin.net/registry/entity/ADSB-3


OrgAbuseHandle: AEA8-ARIN
OrgAbuseName:   Amazon EC2 Abuse
OrgAbusePhone:  +1-206-266-4064
OrgAbuseEmail:  abuse@amazonaws.com
OrgAbuseRef:    https://rdap.arin.net/registry/entity/AEA8-ARIN

OrgNOCHandle: AANO1-ARIN
OrgNOCName:   Amazon AWS Network Operations
OrgNOCPhone:  +1-206-266-4064
OrgNOCEmail:  amzn-noc-contact@amazon.com
OrgNOCRef:    https://rdap.arin.net/registry/entity/AANO1-ARIN

OrgTechHandle: ANO24-ARIN
OrgTechName:   Amazon EC2 Network Operations
OrgTechPhone:  +1-206-266-4064
OrgTechEmail:  amzn-noc-contact@amazon.com
OrgTechRef:    https://rdap.arin.net/registry/entity/ANO24-ARIN

# end


# start

NetRange:       18.128.0.0 - 18.255.255.255
CIDR:           18.128.0.0/9
NetName:        AT-88-Z
NetHandle:      NET-18-128-0-0-1
Parent:         NET18 (NET-18-0-0-0-0)
NetType:        Direct Allocation
OriginAS:
Organization:   Amazon Technologies Inc. (AT-88-Z)
RegDate:        2018-06-29
Updated:        2018-09-19
Ref:            https://rdap.arin.net/registry/ip/18.128.0.0
```

```
Domain Name: foxflores.com
Registry Domain ID: 2120056916_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: http://www.godaddy.com
Updated Date: 2019-04-16T13:03:50Z
Creation Date: 2017-05-03T14:04:14Z
Registrar Registration Expiration Date: 2021-05-03T14:04:14Z
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
Registrant Organization: Fox flores
Registrant State/Province: Minas Gerais
Registrant Country: BR
Registrant Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=foxfl
ores.com
Admin Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=foxflores.
com
Tech Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=foxflores.c
om
Name Server: NS01.DOMAINCONTROL.COM
Name Server: NS02.DOMAINCONTROL.COM
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
```

```
Domain Name: sstawebm.com
Registry Domain ID: 2480083236_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: http://www.godaddy.com
Updated Date: 2020-01-14T17:08:27Z
Creation Date: 2020-01-14T17:08:26Z
Registrar Registration Expiration Date: 2021-01-14T17:08:26Z
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
Registrant Organization:
Registrant State/Province: Puerto Rico
Registrant Country: US
Registrant Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=sstawebm.com
Admin Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=sstawebm.com
Tech Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=sstawebm.com
Name Server: NS51.DOMAINCONTROL.COM
Name Server: NS52.DOMAINCONTROL.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: 2020.01.15 08:46:39 -03'00'