

Alerta de seguridad informática	8FFR-00126-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	25 de Noviembre de 2019
Última revisión	25 de Noviembre de 2019

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 loC 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 loC 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 asociados a una IP que clonan 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:

[http://glovalcoin\[.\]site/owner/imagenes/comun2008/banca-en-linea-personas\[.\]html](http://glovalcoin[.]site/owner/imagenes/comun2008/banca-en-linea-personas[.]html)

[http://www\[.\]nailloungebypinky\[.\]com/wp-](http://www[.]nailloungebypinky[.]com/wp-content/www[.]bancoestado[.]cl/imagenes/comun2008/banca-en-linea-personas[.]html)

[content/www\[.\]bancoestado\[.\]cl/imagenes/comun2008/banca-en-linea-personas\[.\]html](http://www[.]bancoestado[.]cl/imagenes/comun2008/banca-en-linea-personas[.]html)

Network information	
IP address	23.254.253.92
Location	Seattle, Washington, United States (US) 
Registry	arin
Reverse DNS (PTR record)	informatica.ms
ASN number	<u>54290</u>
ASN name (ISP)	Hostwinds LLC.
IP-range/subnet	<u>23.254.128.0/17</u> 23.254.128.0 - 23.254.255.255

Domain nailloungebypinky.com																	
nailloungebypinky / com / Subdomains																	
record type	TTL	value															
A	10800	160.153.129.229															
NS	3600	ns76.domaincontrol.com	Zones on DNS server 173.201.75.48														
NS	3600	ns75.domaincontrol.com	Zones on DNS server 97.74.107.48														
SOA	3600	<table border="1"> <tr> <td>Mname</td> <td>ns75.domaincontrol.com</td> </tr> <tr> <td>Rname</td> <td>dns.jomax.net</td> </tr> <tr> <td>Serial number</td> <td>2019100602</td> </tr> <tr> <td>Refresh</td> <td>28800</td> </tr> <tr> <td>Retry</td> <td>7200</td> </tr> <tr> <td>Expire</td> <td>604800</td> </tr> <tr> <td>Minimum TTL</td> <td>600</td> </tr> </table>		Mname	ns75.domaincontrol.com	Rname	dns.jomax.net	Serial number	2019100602	Refresh	28800	Retry	7200	Expire	604800	Minimum TTL	600
Mname	ns75.domaincontrol.com																
Rname	dns.jomax.net																
Serial number	2019100602																
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

Criteria
Identity = 'glovalcoin.site'

Certificates
None found

		Criteria	Identity = 'www.nailloungebypinky.com'		
Certificates	crt.sh ID	Logged At	Not Before	Not After	Issuer Name
		100015445	2017-03-07	2017-03-05	2017-06-03
	73829286	2017-01-06	2017-01-03	2017-04-03	C=US, ST=TX, L=Houston, O="cPanel, Inc.", CN="cPanel, Inc. Certification Authority"

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

IP

23.254.254.92

160.153.129.229

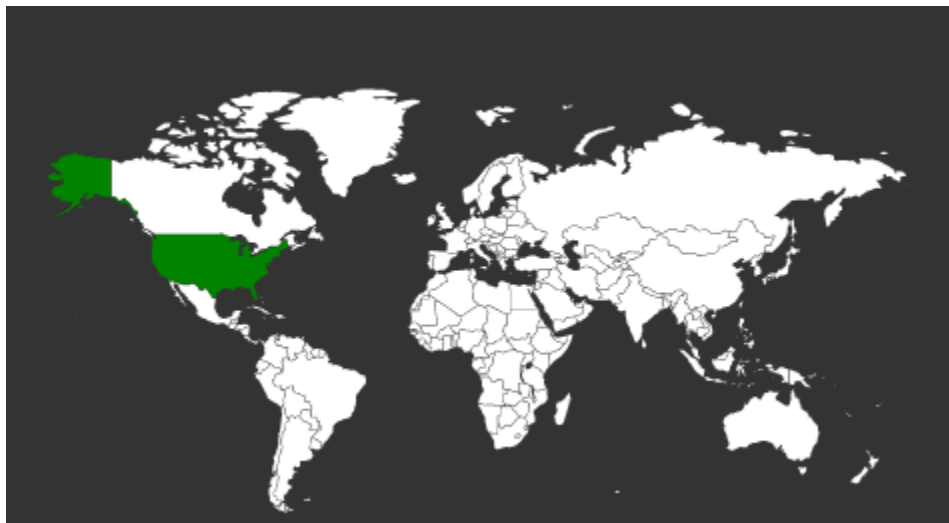
Domain <u>nailloungebypinky.com</u> is located on IP address << 160.153.129.229 >>	
Block start	160.153.0.0
End of block	160.153.255.255
Block size	65536 Domains in block
Block name	GO-DADDY-COM-LLC
AS number	26496
Parent block	160.0.0.0 - 160.255.255.255
Organization	GoDaddy.com, LLC
City	Scottsdale
Region/State	Arizona
Country	US , United States
Reg. date	2011-09-01
Host name	ip-160-153-129-229.ip.secureserver.net
Web server	Apache/2.4.23
Domain count	>= 722 Servers around
Domains	<ol style="list-style-type: none"> 1 *.blac.com 2 1300awful.com 3 1stopvitaminshop.com 4 802banchi.jp 5 abm-company.com 6 abmsk.com 7 accountability-madagascar.org 8 acount-manager.org 9 activeprom.com 10 activitesrentables.com

Network information	
IP address	23.254.253.92
Location	Seattle, Washington, United States (US)
Registry	arin
Reverse DNS (PTR record)	informatica.ms
ASN number	54290
ASN name (ISP)	Hostwinds LLC.
IP-range/subnet	23.254.128.0/17 23.254.128.0 - 23.254.255.255

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

Localización

Seattle, Washington, Estados Unidos



Scottsdale, Arizona, Estados Unidos

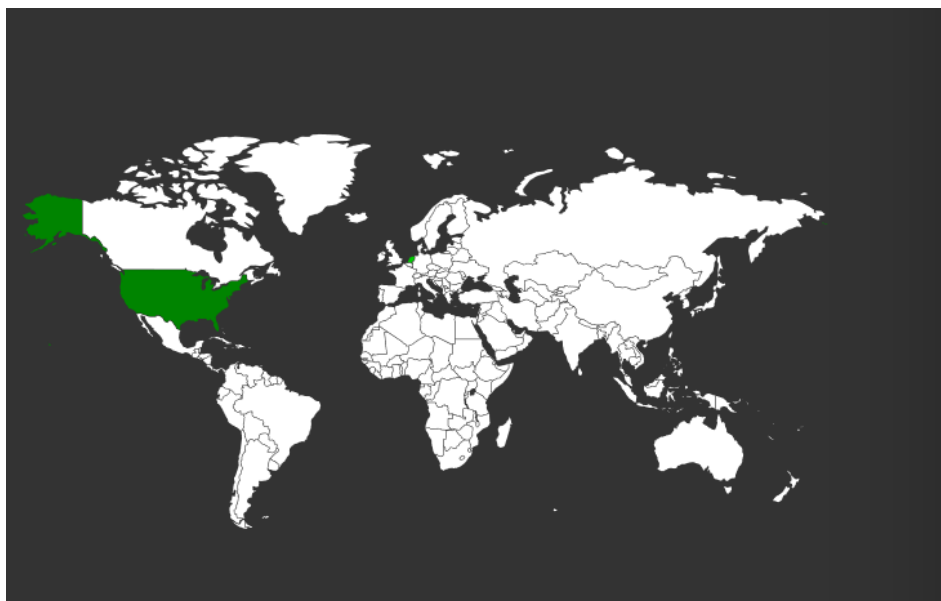
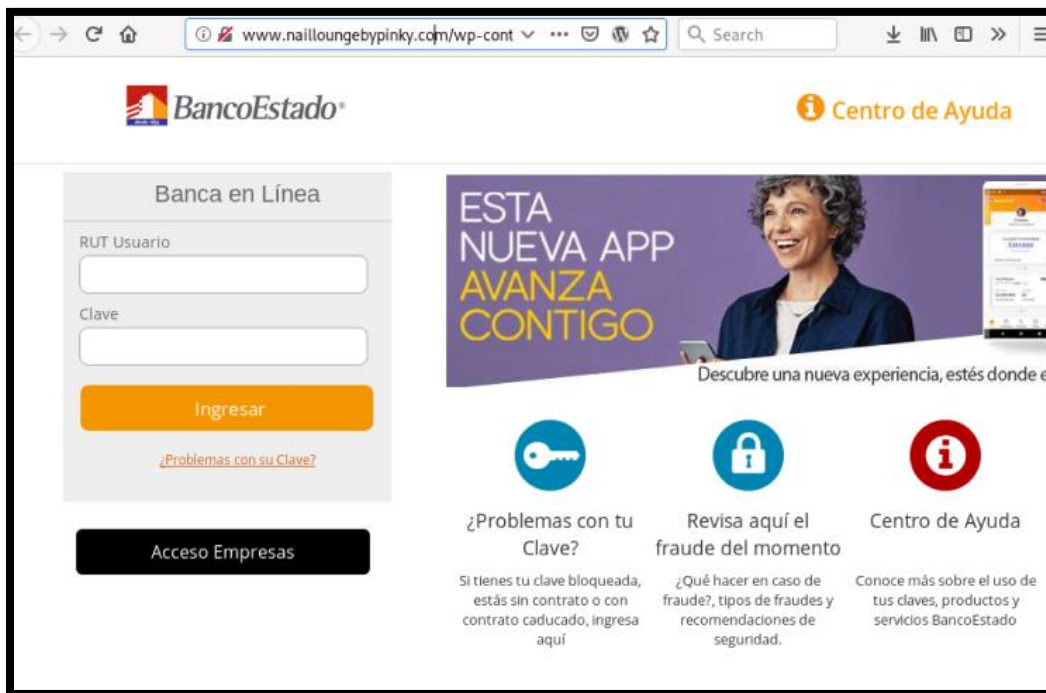
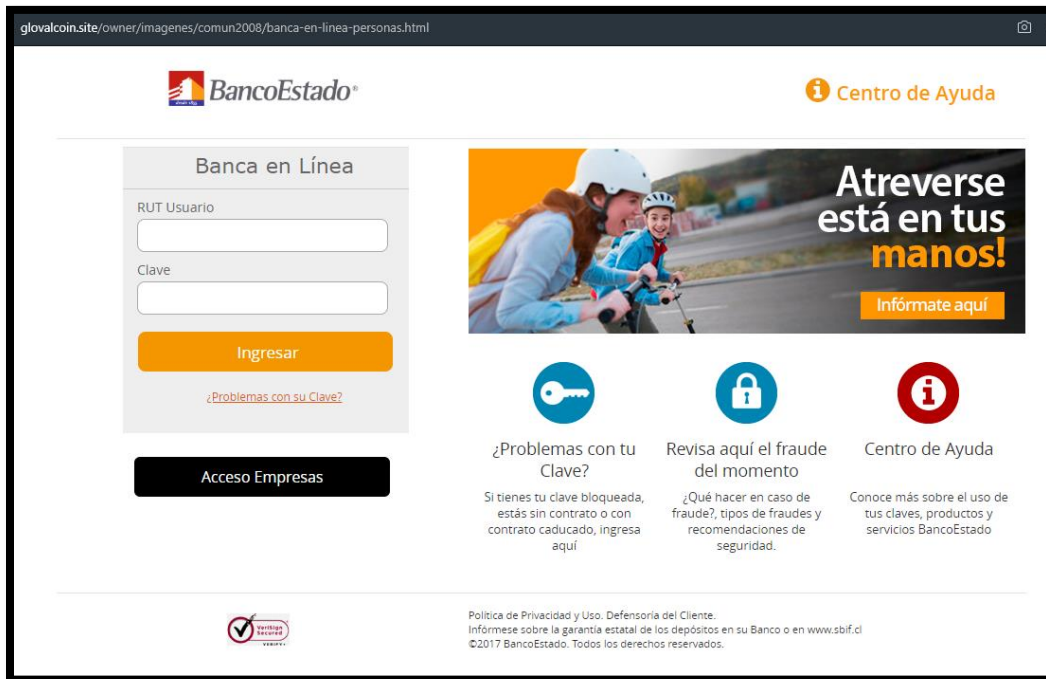


Imagen del sitio



Whois

```
Domain Name: GLOVALCOIN.SITE
Registry Domain ID: D14662903-CHIC
Registrar WHOIS Server: whois.cdmn.com
Registrar URL: https://www.cdmn.com/
Updated Date: 2019-11-20T16:04:59.0Z
Creation Date: 2019-11-20T16:02:57.0Z
Registry Expiry Date: 2020-11-20T23:59:59.0Z
Registrar: I0denochispahard SL (Cdmn)
Registrar IANA ID: 1403
Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: addPeriod https://icann.org/epp#addPeriod
Registrant Organization:
Registrant State/Province:
Registrant Country: PE
Registrant Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name.
Admin Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name.
Tech Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name.
Name Server: DALMS6.MASTERS.COM
Name Server: DALMS6.MASTERS.COM
DNSSEC: unsigned
```

```
Domain Name: nailloungebypinky.com
Registry Domain ID: 2198017334_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: http://www.godaddy.com
Updated Date: 2018-12-10T19:12:31Z
Creation Date: 2017-12-09T19:36:05Z
Registrar Registration Expiration Date: 2019-12-09T19:36:05Z
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: concept Studio
Registrant State/Province: punjab
Registrant Country: PK
Registrant Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=nailloungebypinky.com
Admin Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=nailloungebypinky.com
Tech Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=nailloungebypinky.com
Name Server: NS75.DOMAINCONTROL.COM
Name Server: NS76.DOMAINCONTROL.COM
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2019-11-21T15:00:00Z <<<
```

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