Alerta de seguridad informática	8FFR-00103-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	05 de Noviembre de 2019
Última revisión	05 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 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

URL´s

http[://]scratchpad[.]co[.]in/readme/imagenes/comun2008/banca-en-linea-personas[.]html

Domain scratchpad.co.in

scratchpad / co / in / Subdomains

record type	TTL	value		
A	10800	166.62.28.89		
NS	3600	ns59.domaincontrol.com	Zones on DNS server	97.74.100.31
NS	3600	ns60.domaincontrol.com	Zones on DNS server	173.201.68.31
MX	3600	0 mail.scratchpad.co.in		
TXT	3600	v=spf1 a mx ptr include:secureserver.net ~all		
SOA	3600	Mname: ns59.domaincontrol.com Rname: dns.jomax.net Serial number: 2019031802 Refresh: 28800 Retry: 7200 Expire: 604800 Minimum TTL: 600		

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

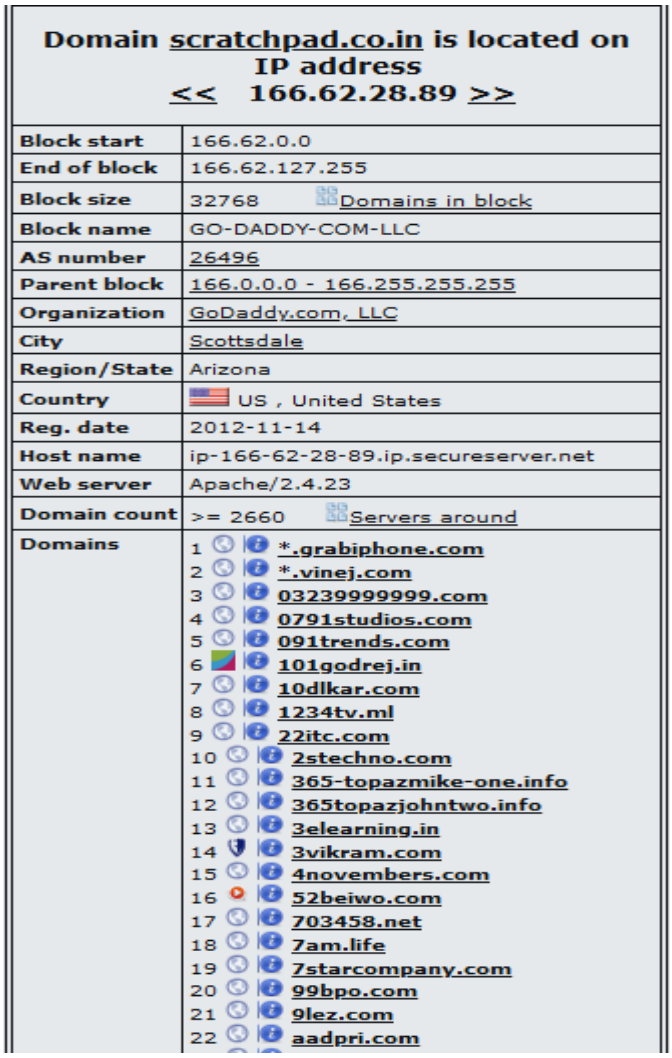
Certificado

Criteria	Identity = 'scratchpad.co.in'
Certificates	*None found*

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

IP´s

166[.]62[.]28[.]89

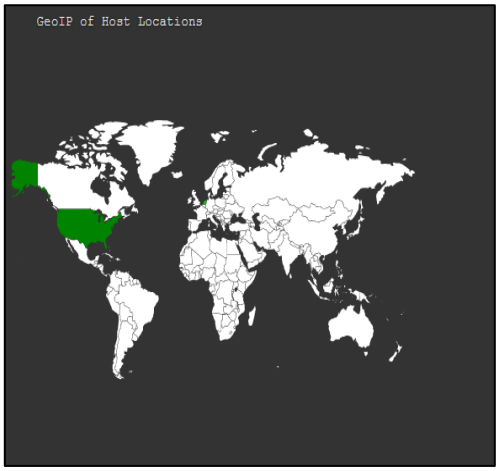


Domain scratchpad.co.in is located on IP address
<< 166.62.28.89 >>

Block start	166.62.0.0
End of block	166.62.127.255
Block size	32768 Domains in block
Block name	GO-DADDY-COM-LLC
AS number	26496
Parent block	166.0.0.0 - 166.255.255.255
Organization	GoDaddy.com, LLC
City	Scottsdale
Region/State	Arizona
Country	US , United States
Reg. date	2012-11-14
Host name	ip-166-62-28-89.ip.secureserver.net
Web server	Apache/2.4.23
Domain count	>= 2660 Servers around
Domains	1 *.grabiphone.com 2 *.vinej.com 3 03239999999.com 4 0791studios.com 5 091trends.com 6 101godrej.in 7 10dlkar.com 8 1234tv.ml 9 22itc.com 10 2stechno.com 11 365-topazmike-one.info 12 365topazjohntwo.info 13 3elearning.in 14 3vikram.com 15 4novembers.com 16 52beiwo.com 17 703458.net 18 7am.life 19 7starcompany.com 20 99bpo.com 21 9lez.com 22 aadpri.com

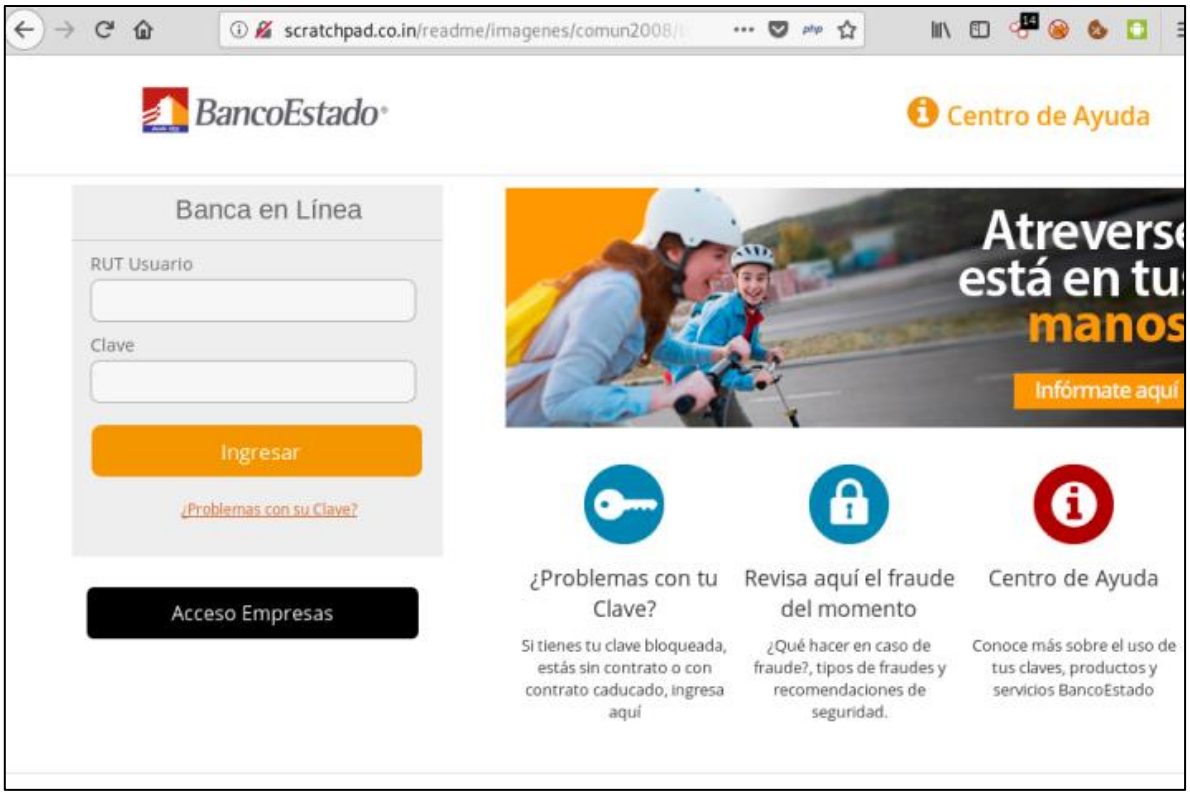
Ilustración 3 Ip de Origen donde se aloja Sitio Falso del Banco Estado

Localización



Estados Unidos, Arizona

Imagen del sitio



Whois

```
Domain Name: scratchpad.co
Registry Domain ID: D1FB9EB2E3546460EB0418999F45CD20E-NSR
Registrar WHOIS Server: whois.domain.com
Registrar URL: www.domain.com
Updated Date: 2019-01-12T17:22:44Z
Creation Date: 2018-01-22T00:14:53Z
Registry Expiry Date: 2020-01-22T00:14:53Z
Registrar: Domain.com, LLC
Registrar IANA ID: 886
Registrar Abuse Contact Email: compliance@domain-inc.net
Registrar Abuse Contact Phone: +1.6022262389
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Registry Registrant ID:
Registrant Name:
Registrant Organization: Scratchpad Creative Inc.
Registrant Street:
Registrant Street:
Registrant Street:
Registrant City:
Registrant State/Province: BC
Registrant Postal Code:
Registrant Country: CA
Registrant Phone:
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: Please query the RDDS service of the Registrar of Record identified in this output for infor
mation on how to contact the Registrant, Admin, or Tech contact of the queried domain name.
Registry Admin ID:
Admin Name:
Admin Organization:
Admin Street:
Admin Street:
Admin Street:
Admin City:
Admin State/Province:
Admin Postal Code:
Admin Country:
Admin Phone:
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: Please query the RDDS service of the Registrar of Record identified in this output for informatio
n on how to contact the Registrant, Admin, or Tech contact of the queried domain name.
Registry Tech ID:
Tech Name:
Tech Organization:
Tech Street:
Tech Street:
Tech Street:
Tech City:
Tech State/Province:
Tech Postal Code:
Tech Country:
Tech Phone:
Tech Phone Ext:
Tech Fax:
Tech Fax Ext:
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: ns2.spcr.ca
```

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: 2019.11.05 08:08:07 -03'00'