Alerta de seguridad informática	8FFR-00111-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de Noviembre de 2019
Última revisión	14 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.

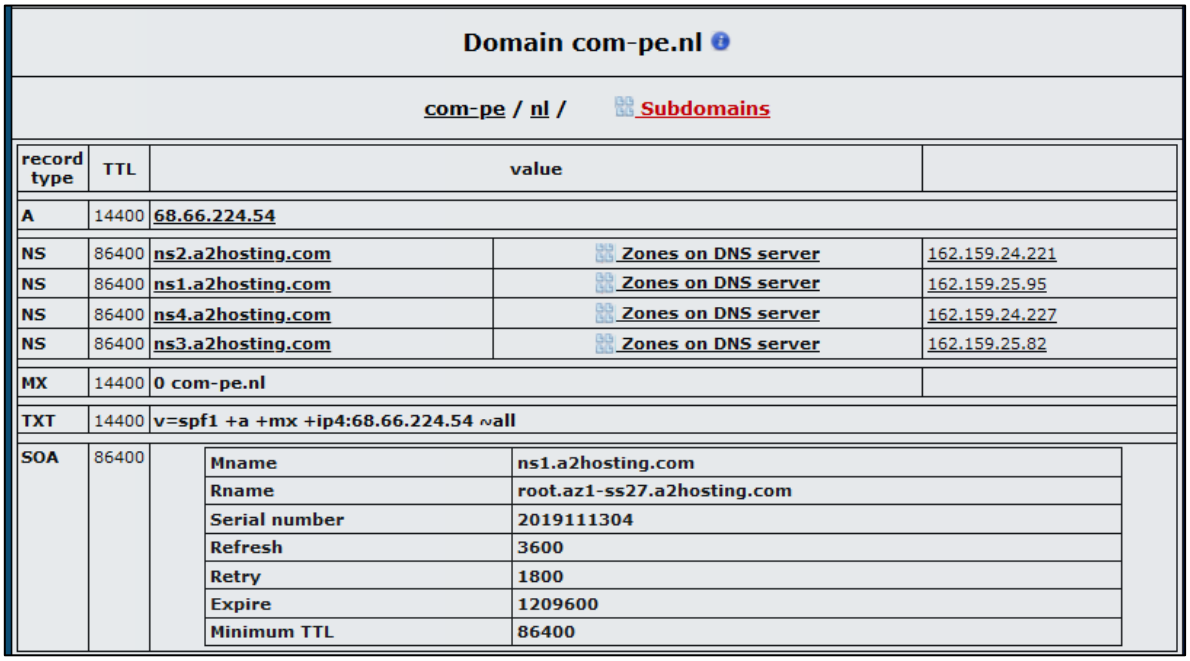
Lo anterior constituye una falsificación de la marca institucional que podría afectar a usuarios, clientes y a la entidad bancaria aludida.

Indicadores de Compromisos

URL´s

https[://]www[.]bancaestado[.]com-pe[.]nl/imagenes/comun2008/banca-en-linea-personas[.]html

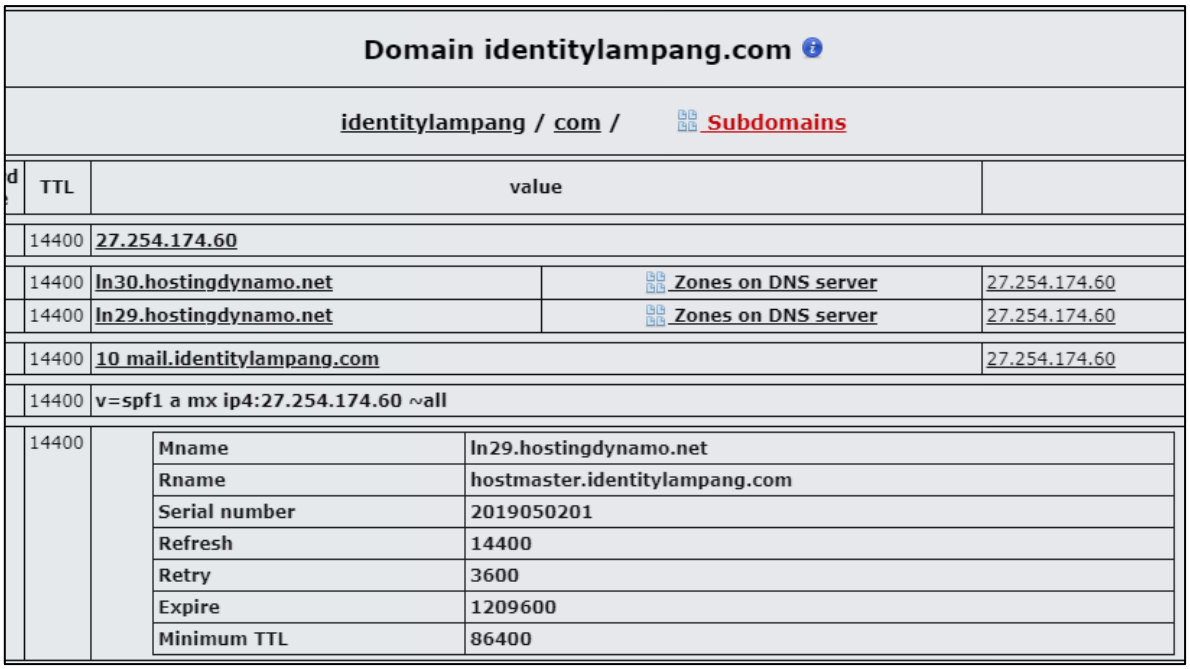
http[://]identitylampang[.]com/include/www[.]bancoestado[.]cl/imagenes/comun2008/banca-en-linea-personas[.]html



Domain com-pe.nl

com-pe / nl / Subdomains

record type	TTL	value		
A	14400	68.66.224.54		
NS	86400	ns2.a2hosting.com	Zones on DNS server	162.159.24.221
NS	86400	ns1.a2hosting.com	Zones on DNS server	162.159.25.95
NS	86400	ns4.a2hosting.com	Zones on DNS server	162.159.24.227
NS	86400	ns3.a2hosting.com	Zones on DNS server	162.159.25.82
MX	14400	0 com-pe.nl		
TXT	14400	v=spf1 +a +mx +ip4:68.66.224.54 ~all		
SOA	86400	Mname: ns1.a2hosting.com Rname: root.az1-ss27.a2hosting.com Serial number: 2019111304 Refresh: 3600 Retry: 1800 Expire: 1209600 Minimum TTL: 86400		



Domain identitylampang.com

identitylampang / com / Subdomains

d	TTL	value		
	14400	27.254.174.60		
	14400	ln30.hostingdynamo.net	Zones on DNS server	27.254.174.60
	14400	ln29.hostingdynamo.net	Zones on DNS server	27.254.174.60
	14400	10 mail.identitylampang.com		27.254.174.60
	14400	v=spf1 a mx ip4:27.254.174.60 ~all		
	14400	Mname: ln29.hostingdynamo.net Rname: hostmaster.identitylampang.com Serial number: 2019050201 Refresh: 14400 Retry: 3600 Expire: 1209600 Minimum TTL: 86400		

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

Certificado

Criteria	Identity = 'com-pe.nl'

Certificates

crt.sh ID	Logged At	Not Before	Not After	Issuer Name
2003576138	2019-10-16	2019-10-16	2020-01-14	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
2003565621	2019-10-16	2019-10-16	2020-01-14	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3

Criteria	Identity = 'identitylampang.com'

Certificates

crt.sh ID	Logged At	Not Before	Not After	Issuer Name
2064388322	2019-11-02	2019-11-02	2020-01-31	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
2064388227	2019-11-02	2019-11-02	2020-01-31	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1861021205	2019-09-03	2019-09-03	2019-12-02	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1841967215	2019-09-03	2019-09-03	2019-12-02	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1654887590	2019-07-05	2019-07-05	2019-10-03	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1642011854	2019-07-05	2019-07-05	2019-10-03	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3

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

IP´s

68[.]66[.]224[.]154

27[.]254[.]174[.]60

Domain com-pe.nl is located on IP address
<< 68.66.224.54 >>

Block start	68.66.192.0
End of block	68.66.255.255
Block size	16384 Domains in block
Block name	RSN-4
AS number	55293
Parent block	68.0.0.0 - 68.255.255.255
Organization	RockSolid Network, Inc.
City	Ann Arbor
Region/State	Michigan
Country	US , United States
Reg. date	2009-09-01
Host name	az1-ss27.a2hosting.com
Domains	1 com-pe.nl

Domain identitylampang.com is located on IP address
<< 27.254.174.60 >>

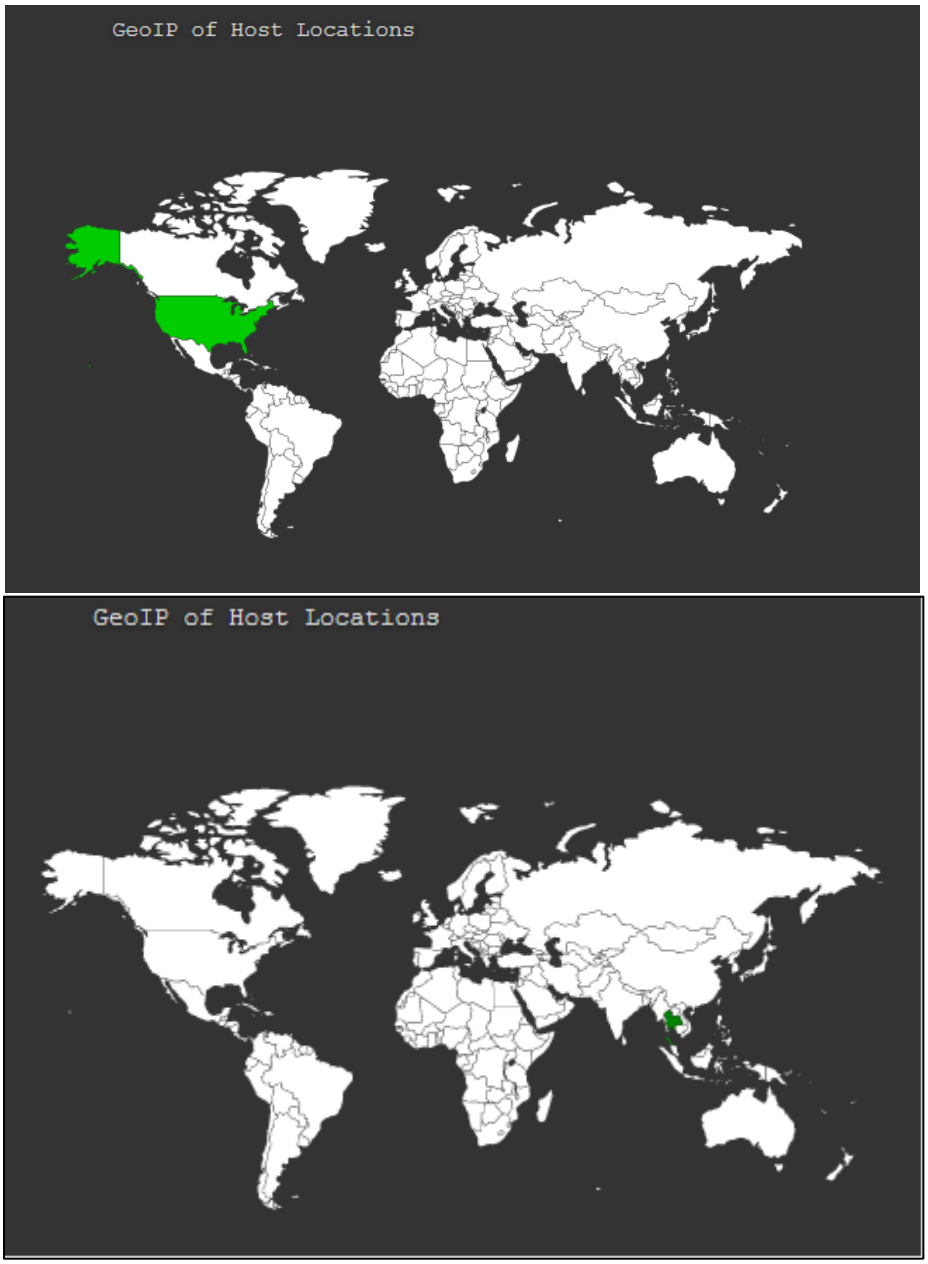
Block start	27.254.174.0
End of block	27.254.174.255
Block size	256 Domains in block
Block name	idc-csloxinfo
AS number	9891
Parent block	27.254.0.0 - 27.254.255.255
Organization	reassign to "CSLOXINFO-IDC" contact *
City	Bangkok
Region/State	Krung Thep Maha Nakhon
Country	TH , Thailand
Host name	ln29.hostingdynamo.net

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

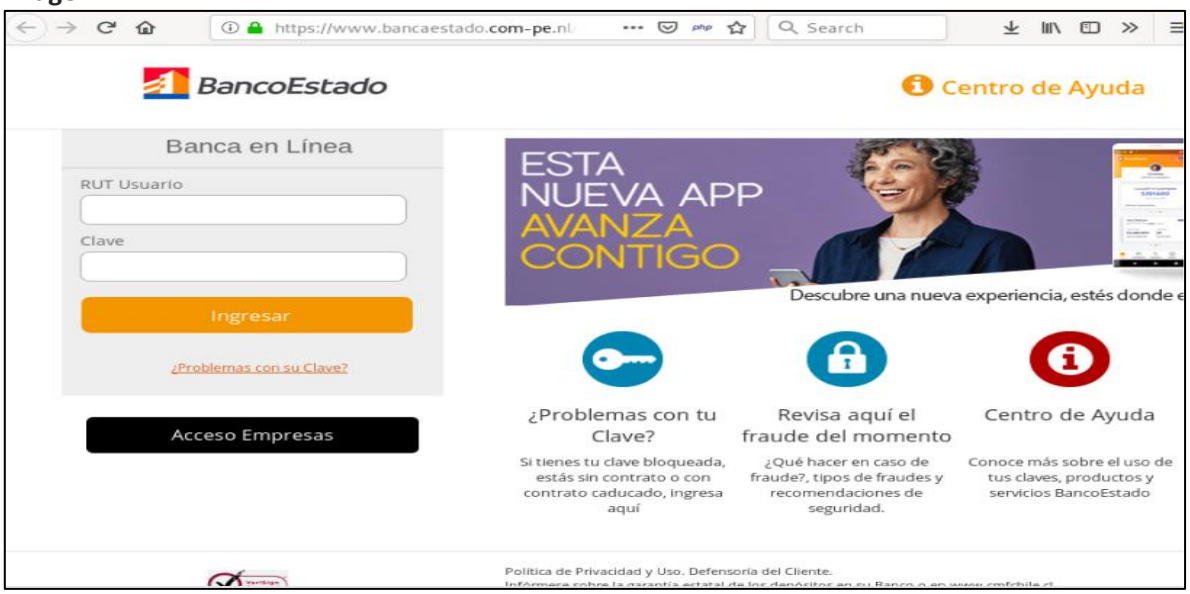
Localización

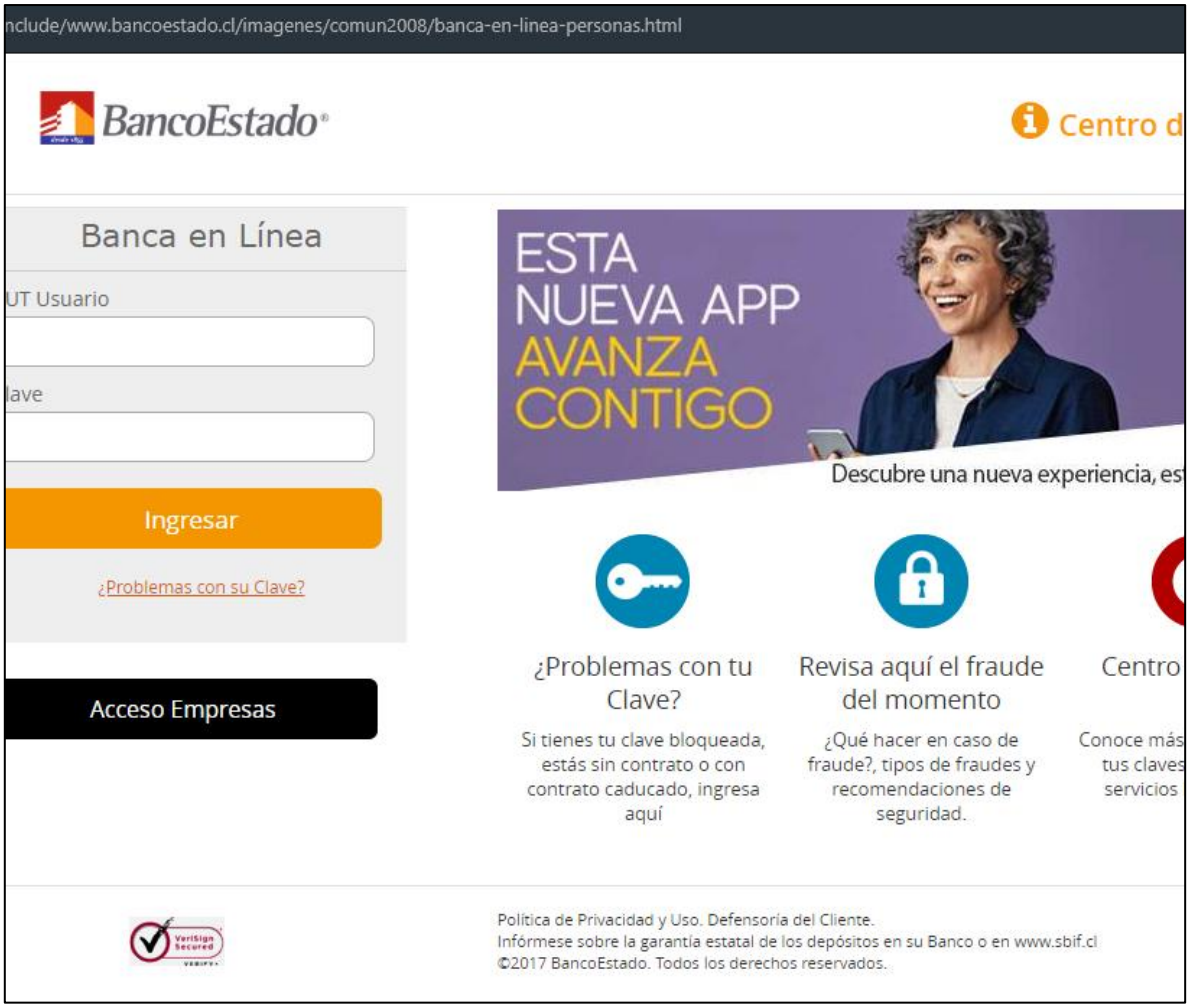
Ann Arbor, Michigan, Estados Unidos

Bangkok, Krung Thep Maha Nakhon, Tailandia



Imagen


https://www.bancaestado.com-pe.nl
Search
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
¿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.


nclude/www.bancoestado.cl/imagenes/comun2008/banca-en-linea-personas.html
BancoEstado
Centro d
Banca en Línea
UT Usuario
lave
Ingresar
¿Problemas con su Clave?
Acceso Empresas
ESTA
NUEVA APP
AVANZA
CONTIGO
Descubre una nueva experiencia, es
¿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
Conoce más
tus claves
servicios
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

```
% IANA WHOIS server
% for more information on IANA, visit http://www.iana.org
% This query returned 1 object

refer:        whois.domain-registry.nl

domain:       NL

organisation: SIDN (Stichting Internet  Domeinregistratie Nederland)
address:      P.O. Box 5022
address:      Arnhem  6802 EA
address:      Netherlands

contact:      administrative
name:         Managing Director
organisation: SIDN (Stichting Internet  Domeinregistratie Nederland)
address:      P.O. Box 5022
address:      Arnhem  6802 EA
address:      Netherlands
phone:        +31 26 3525500
fax-no:       +31 26 3525505
e-mail:       admin@sidn.nl

contact:      technical
name:         Manager ICT
organisation: SIDN (Stichting Internet  Domeinregistratie Nederland)
address:      P.O. Box 5022
address:      Arnhem  6802 EA
address:      Netherlands
phone:        +31 26 3525500
fax-no:       +31 26 3525550
e-mail:       tech@sidn.nl

nserver:      NS1.DNS.NL 194.0.28.53 2001:678:2c:0:194:0:28:53
nserver:      NS2.DNS.NL 194.146.106.42 2001:67c:1010:10:0:0:0:53
nserver:      NS3.DNS.NL 194.0.25.24 2001:678:20:0:0:0:0:24
nserver:      SNS-PB.ISC.ORG 192.5.4.1 2001:500:2e:0:0:0:0:1
ds-rdata:     34112 8 2 3c5b5f9b3557455c50751a9be9ebe9238c88e19f5f07f930976917b5
1b95cd22

whois:        whois.domain-registry.nl

status:       ACTIVE
remarks:      Registration information: https://www.sidn.nl/

created:      1986-04-25
changed:      2018-05-04
source:       IANA

Domain name: com-pe.nl
Status:      active

Registrar:
   E-nom Inc
   5808 Lake Washington Boulevard NE
   Suite 201
   98033 Kirkland
```

```
Domain Name: IDENTITYLAMPANG.COM
Registry Domain ID: 2386633424_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.publicdomainregistry.com
Registrar URL: www.publicdomainregistry.com
Updated Date: 2019-07-02T02:21:51Z
Creation Date: 2019-05-02T03:29:22Z
Registrar Registration Expiration Date: 2020-05-02T03:29:22Z
Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com
Registrar IANA ID: 303
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProh
ibited
Registry Registrant ID: Not Available From Registry
Registrant Name: Ratthasit Yajor
Registrant Organization: Ratthasit Yajor
Registrant Street: 173 0
Registrant City: Muang
Registrant State/Province: Lampang
Registrant Postal Code: 52100
Registrant Country: TH
Registrant Phone: +66.810305262
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: ratthasit.it@gmail.com
Registry Admin ID: Not Available From Registry
Admin Name: Ratthasit Yajor
Admin Organization: Ratthasit Yajor
Admin Street: 173 0
Admin City: Muang
Admin State/Province: Lampang
Admin Postal Code: 52100
Admin Country: TH
Admin Phone: +66.810305262
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: ratthasit.it@gmail.com
Registry Tech ID: Not Available From Registry
Tech Name: Ratthasit Yajor
Tech Organization: Ratthasit Yajor
Tech Street: 173 0
Tech City: Muang
Tech State/Province: Lampang
Tech Postal Code: 52100
Tech Country: TH
Tech Phone: +66.810305262
Tech Phone Ext:
Tech Fax:
Tech Fax Ext:
Tech Email: ratthasit.it@gmail.com
Name Server: ln29.hostingdynamo.net
Name Server: ln30.hostingdynamo.net
DNSSEC: Unsigned
Registrar Abuse Contact Email: abuse-contact@publicdomainregistry.com
Registrar Abuse Contact Phone: +1.2013775952
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2019-11-14T15:51:07Z <<<

For more information on Whois status codes, please visit https://icann.org/epp

Registration Service Provided By: HOSTINGDYNAMO.COM
```

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: 2019.11.14 16:00:43 -03'00'