Alerta de seguridad informática	**8FFR-00083-001**
Clase de alerta	**Fraude**
Tipo de incidente	**Falsificación de Registros o Identidad**
Nivel de riesgo	**Alto**
TLP	**Blanco**
Fecha de lanzamiento original	**09 de Octubre de 2019**
Última revisión	**09 de Octubre 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 redirige a sitios que suplantan el sitio web oficial de **Banco Estado**, lo 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

URL Sitio Clonado:

http[://]bancooestado[.]xyz/imagenes/comun2009/en-linea-personas[.]php

https[://]marketingdigital101[.]com[.]br/Bancoestado/

https[://]www[.]bancooestadoocl[.]xyz/imagenes/comun2009/en-linea-personas[.]php

Domain bancooestado.xyz

bancooestado / xyz / Subdomains

record type	TTL	value		
A	7207	157.245.141.92		
NS	172800	ns1.dnsowl.com	Zones on DNS server	185.34.216.159, 198.251.84.16, 104.207.141.138
NS	172800	ns2.dnsowl.com	Zones on DNS server	168.235.75.52, 64.32.22.100, 45.32.237.128
NS	172800	ns3.dnsowl.com	Zones on DNS server	45.63.106.63, 209.141.39.150, 45.63.5.234

SOA	172800	Mname	ns1.dnsowl.com
		Rname	hostmaster.dnsowl.com
		Serial number	1570473578
		Refresh	7200
		Retry	1800
		Expire	1209600
		Minimum TTL	600

Domain marketingdigital101.com.br

marketingdigital101 / com / br / Subdomains

record type	TTL	value		
A	14400	162.241.178.211		
NS	86400	ns1.ozllo.com.br	Zones on DNS server	162.241.178.211
NS	86400	ns2.ozllo.com.br	Zones on DNS server	162.241.45.209
MX	14400	0 marketingdigital101.com.br		
TXT	14400	v=spf1 +a +mx +ip4:162.241.178.211 ~all		

SOA	86400	Mname	ns1.ozllo.com.br
		Rname	root.vps.4343984.ozllo.com.br
		Serial number	2019082705
		Refresh	3600
		Retry	1800
		Expire	1209600
		Minimum TTL	86400

Domain bancooestadoocl.xyz

bancooestadoocl / xyz / Subdomains

record type	TTL	value		
A	7207	174.138.45.87		
NS	172800	ns1.dnsowl.com	Zones on DNS server	104.207.141.138, 198.251.84.16, 185.34.216.159
NS	172800	ns2.dnsowl.com	Zones on DNS server	45.32.237.128, 168.235.75.52, 64.32.22.100
NS	172800	ns3.dnsowl.com	Zones on DNS server	45.63.5.234, 209.141.39.150, 45.63.106.63
SOA	172800	Mname	ns1.dnsowl.com	
		Rname	hostmaster.dnsowl.com	
		Serial number	1570538989	
		Refresh	7200	
		Retry	1800	
		Expire	1209600	
		Minimum TTL	600	

Ilustración 1 Dominio donde se Aloja Url del Banco Estado

IP´s

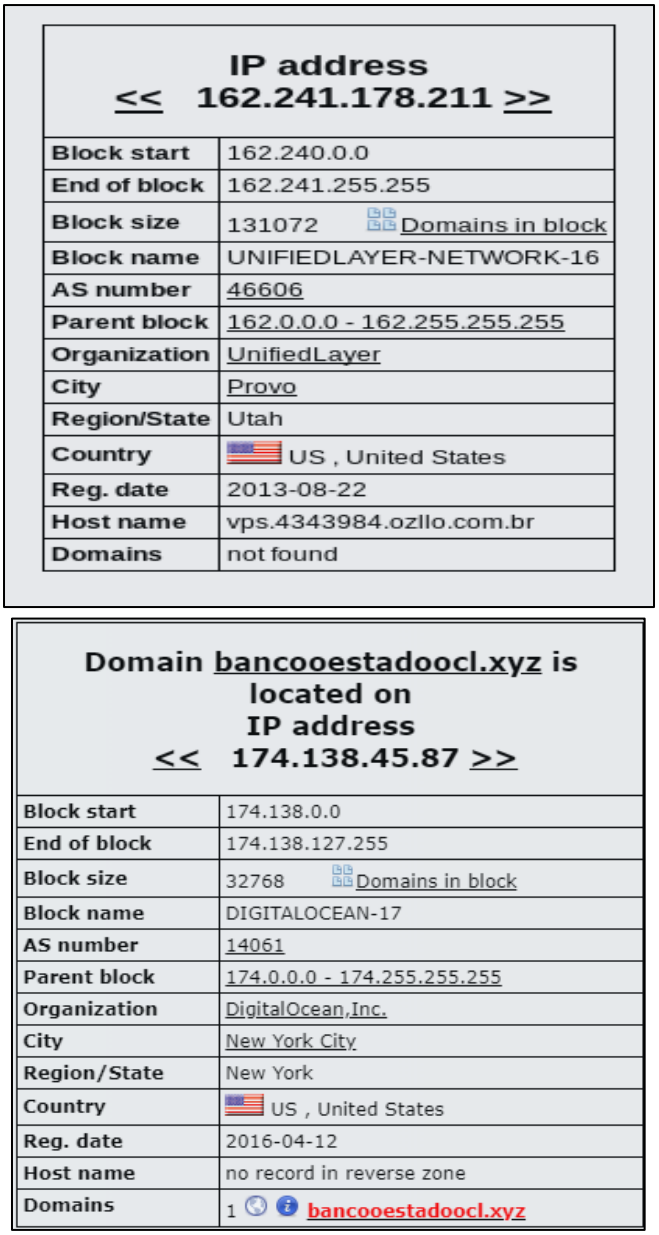
157[.]245[.]141[.]92

162[.]241[.]178[.]211

174[.]138[.]45[.]87

Domain bancooestado.xyz is located on IP address << 157.245.141.92 >>

Block start	157.245.0.0
End of block	157.245.255.255
Block size	65536 Domains in block
Block name	SPSS3
AS number	14061
Parent block	157.0.0.0 - 157.255.255.255
Organization	Datalogic ADC, Inc.
City	Eugene
Region/State	Oregon
Country	US , United States
Reg. date	1992-02-06
Host name	no record in reverse zone
Domains	1 bancooestado.xyz



IP address
<< 162.241.178.211 >>

Block start	162.240.0.0
End of block	162.241.255.255
Block size	131072 Domains in block
Block name	UNIFIEDLAYER-NETWORK-16
AS number	46606
Parent block	162.0.0.0 - 162.255.255.255
Organization	UnifiedLayer
City	Provo
Region/State	Utah
Country	US , United States
Reg. date	2013-08-22
Host name	vps.4343984.ozllo.com.br
Domains	not found

Domain bancooestadoocl.xyz is located on IP address
<< 174.138.45.87 >>

Block start	174.138.0.0
End of block	174.138.127.255
Block size	32768 Domains in block
Block name	DIGITALOCEAN-17
AS number	14061
Parent block	174.0.0.0 - 174.255.255.255
Organization	DigitalOcean,Inc.
City	New York City
Region/State	New York
Country	US , United States
Reg. date	2016-04-12
Host name	no record in reverse zone
Domains	1 bancooestadoocl.xyz

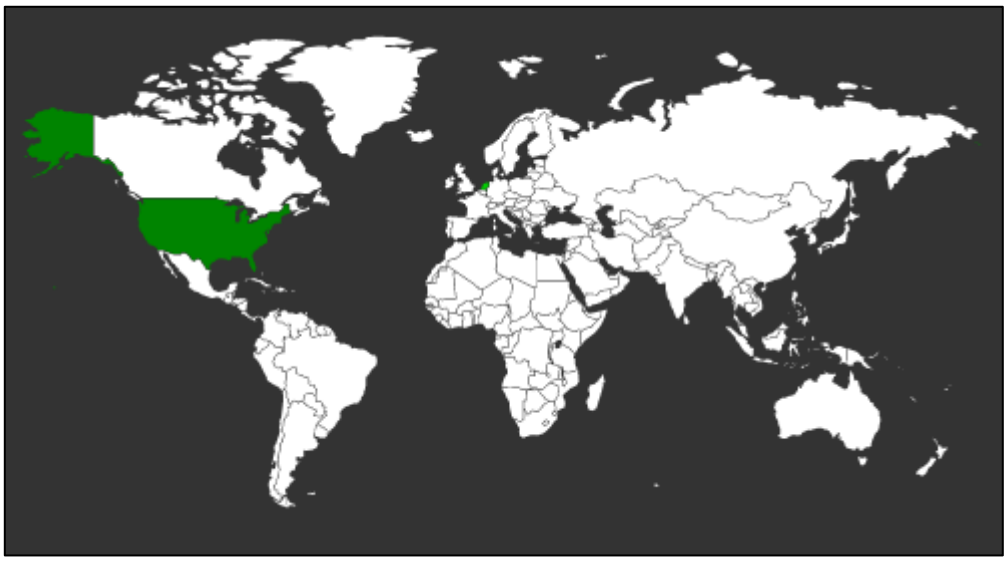
Ilustración 2 Ip de Origen donde se aloja Sitio Falso del Banco Estado

Localización

North Bergen, New Jersey, Estados Unidos

Provo, Utah, Estados Unidos

New York City, Estados Unidos



Certificados

Certificates

crt.sh ID	Logged At ⇧	Not Before	Not After	Issuer Name
1964509856	2019-10-05	2019-10-05	2020-01-03	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1964509842	2019-10-05	2019-10-05	2020-01-03	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3

Criteria: Identity = 'marketingdigital101.com.br'

Certificates

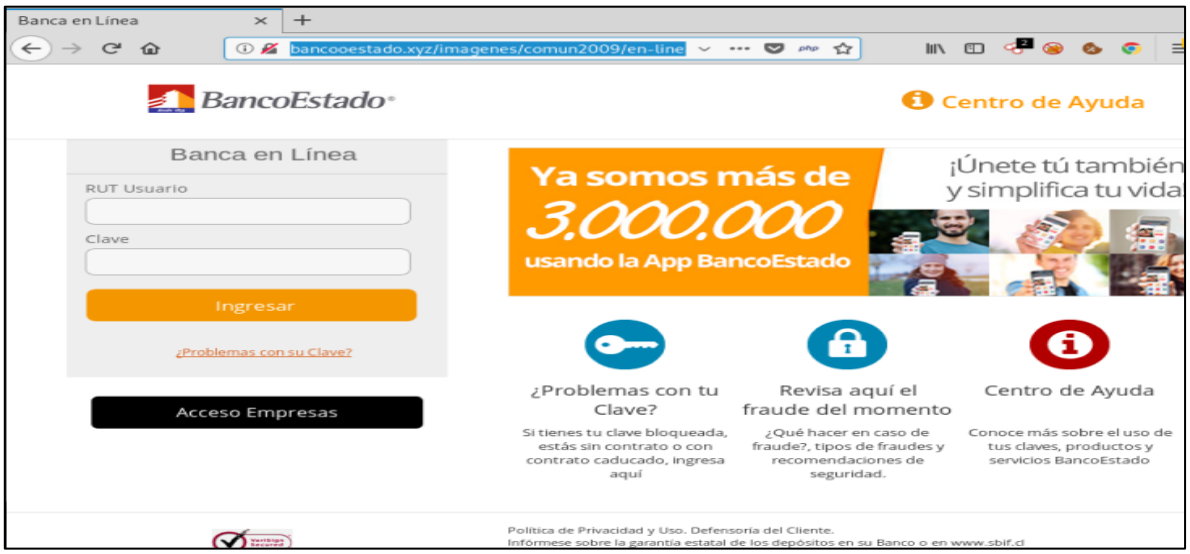
crt.sh ID	Logged At ⇧	Not Before	Not After	Issuer Name
1856361091	2019-08-27	2019-08-27	2019-11-25	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1815703035	2019-08-27	2019-08-27	2019-11-25	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3

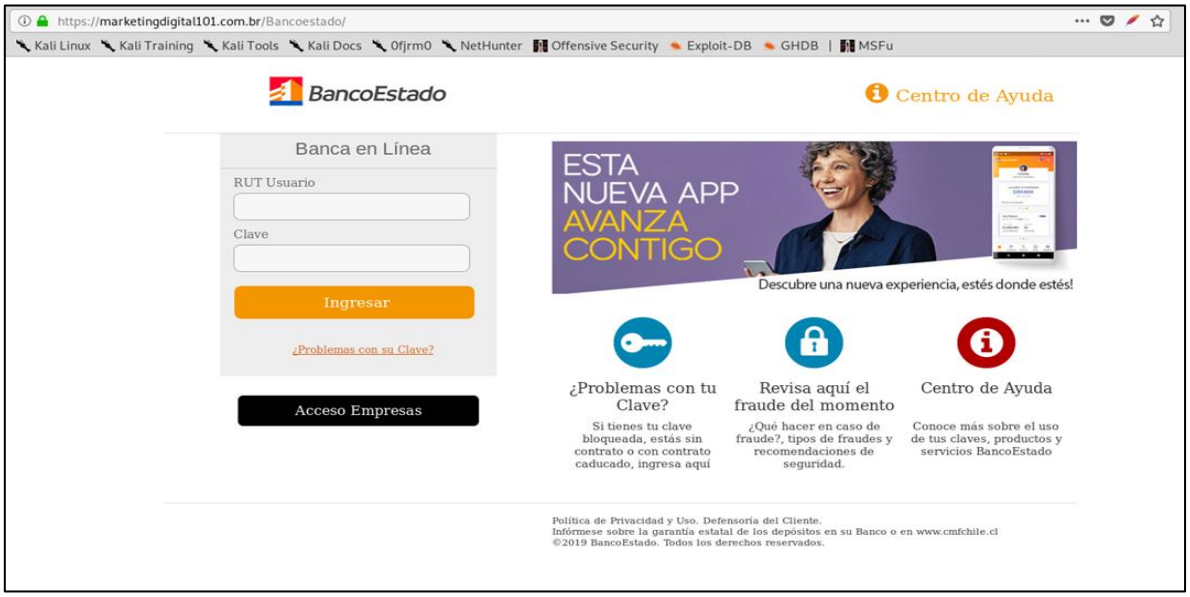
Certificates

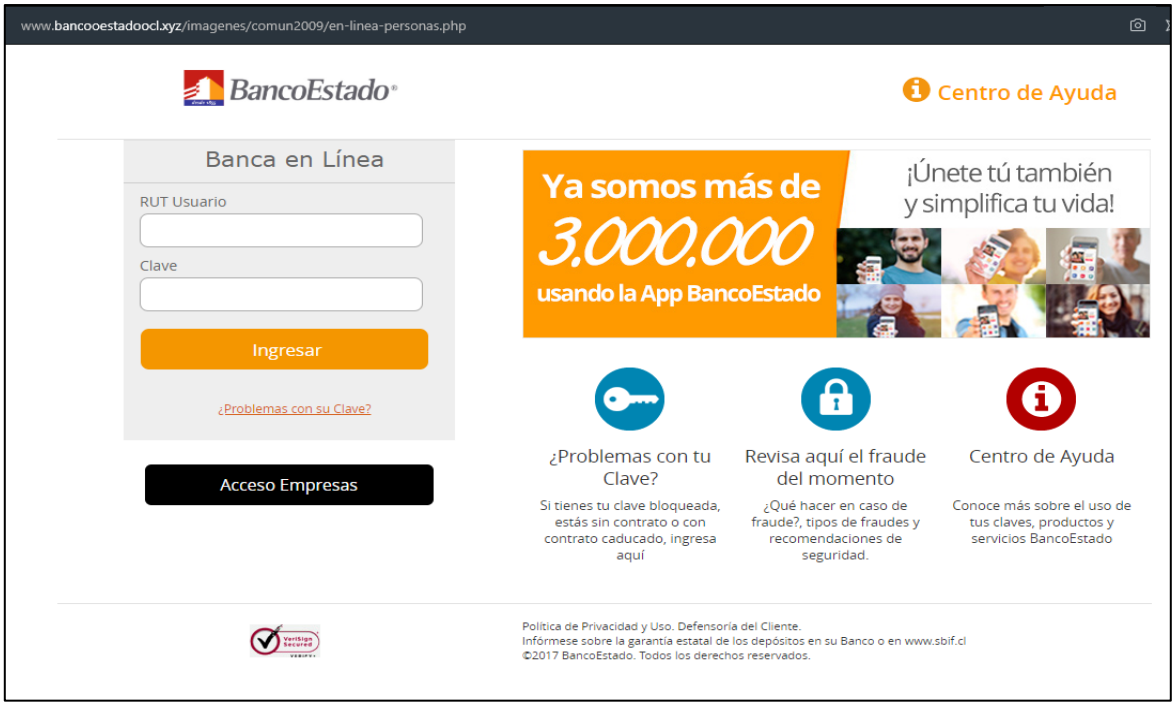
crt.sh ID	Logged At ⇧	Not Before	Not After	Issuer Name
1973253083	2019-10-08	2019-10-08	2020-01-06	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3

Ilustración 3 Certificado Utilizado en Url del sitio Falso del Banco Estado

Imagen del sitio







Whois

```
Domain Name: bancooestado.xyz
Registry Domain ID: D133269281-CNIC
Registrar WHOIS Server: whois.namesilo.com
Registrar URL: https://www.namesilo.com/
Updated Date: 2019-10-06T07:00:00Z
Creation Date: 2019-10-05T07:00:00Z
Registrar Registration Expiration Date: 2020-10-05T07:00:00Z
Registrar: NameSilo, LLC
Registrar IANA ID: 1479
Registrar Abuse Contact Email: abuse@namesilo.com
Registrar Abuse Contact Phone: +1.4805240066
Domain Status: clientTransferProhibited https://www.icann.org/epp#clientTransferProhibited
Registry Registrant ID:
Registrant Name: Domain Administrator
Registrant Organization: See PrivacyGuardian.org
Registrant Street: 1928 E. Highland Ave. Ste F104 PMB# 255
Registrant City: Phoenix
Registrant State/Province: AZ
Registrant Postal Code: 85016
Registrant Country: US
Registrant Phone: +1.3478717726
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: pw-a0589lcb7be2c75ebcbc69662097blca@privacyguardian.org
Registry Admin ID:
Admin Name: Domain Administrator
Admin Organization: See PrivacyGuardian.org
Admin Street: 1928 E. Highland Ave. Ste F104 PMB# 255
Admin City: Phoenix
Admin State/Province: AZ
Admin Postal Code: 85016
Admin Country: US
Admin Phone: +1.3478717726
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: pw-a0589lcb7be2c75ebcbc69662097blca@privacyguardian.org
Registry Tech ID:
Tech Name: Domain Administrator
Tech Organization: See PrivacyGuardian.org
Tech Street: 1928 E. Highland Ave. Ste F104 PMB# 255
Tech City: Phoenix
Tech State/Province: AZ
Tech Postal Code: 85016
Tech Country: US
Tech Phone: +1.3478717726
Tech Phone Ext:
Tech Fax:
Tech Fax Ext:
Tech Email: pw-a0589lcb7be2c75ebcbc69662097blca@privacyguardian.org
Name Server: NS1.DNSOWL.COM
Name Server: NS2.DNSOWL.COM
Name Server: NS3.DNSOWL.COM
DNSSEC: unsigned
```

```
soc@ITQ-ivps2:~$ whois marketingdigitall01.com.br

% Copyright (c) Nic.br
%  The use of the data below is only permitted as described in
%  full by the terms of use at https://registro.br/termo/en.html ,
%  being prohibited its distribution, commercialization or
%  reproduction, in particular, to use it for advertising or
%  any similar purpose.
%  2019-10-08T09:41:37-03:00

domain:       marketingdigitall01.com.br
owner:        zoe povoa
ownerid:      449.006.308-37
country:      BR
owner-c:      ZOPOV
admin-c:      ZOPOV
tech-c:       ZOPOV
billing-c:    ZOPOV
nserver:      ns1.ozllo.com.br
nsstat:       20191006 AA
nslastaa:     20191006
nserver:      ns2.ozllo.com.br
nsstat:       20191006 AA
nslastaa:     20191006
saci:         yes
created:      20190725 #19932489
changed:      20190827
expires:      20200725
status:       published
provider:     ENDURANCE-BRASIL (43)

nic-hdl-br:   ZOPOV
person:       zoe povoa
e-mail:       zoe.povoa@hotmail.com
country:      BR
created:      20170905
changed:      20170905
```

```
Domain Name: bancooestadoocl.xyz
Registrar WHOIS Server: whois.namesilo.com
Registrar URL: https://www.namesilo.com/
Updated Date: 2019-10-08T07:00:00Z
Creation Date: 2019-10-08T07:00:00Z
Registrar Registration Expiration Date: 2020-10-08T07:00:00Z
Registrar: NameSilo, LLC
Registrar IANA ID: 1479
Registrar Abuse Contact Email: abuse@namesilo.com
Registrar Abuse Contact Phone: +1.4805240066
Domain Status: clientTransferProhibited https://www.icann.org/epp#clientTransferProhibited
Registry Registrant ID:
Registrant Name: Domain Administrator
Registrant Organization: See PrivacyGuardian.org
Registrant Street: 1928 E. Highland Ave. Ste F104 PMB# 255
Registrant City: Phoenix
Registrant State/Province: AZ
Registrant Postal Code: 85016
Registrant Country: US
Registrant Phone: +1.3478717726
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: pw-3c794a363flabe3alfa3f91c6cea3161@privacyguardian.org
Registry Admin ID:
Admin Name: Domain Administrator
Admin Organization: See PrivacyGuardian.org
Admin Street: 1928 E. Highland Ave. Ste F104 PMB# 255
Admin City: Phoenix
Admin State/Province: AZ
Admin Postal Code: 85016
Admin Country: US
Admin Phone: +1.3478717726
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: pw-3c794a363flabe3alfa3f91c6cea3161@privacyguardian.org
Registry Tech ID:
Tech Name: Domain Administrator
Tech Organization: See PrivacyGuardian.org
Tech Street: 1928 E. Highland Ave. Ste F104 PMB# 255
Tech City: Phoenix
Tech State/Province: AZ
Tech Postal Code: 85016
Tech Country: US
Tech Phone: +1.3478717726
Tech Phone Ext:
Tech Fax:
Tech Fax Ext:
Tech Email: pw-3c794a363flabe3alfa3f91c6cea3161@privacyguardian.org
Name Server: NS1.DNSOWL.COM
Name Server: NS2.DNSOWL.COM
Name Server: NS3.DNSOWL.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: 2019.10.09 08:24:45 -03'00'