Alerta de seguridad informática	8FFR20-00232-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	28 de Febrero de 2020
Última revisión	28 de Febrero 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 dos IP que suplantan el sitio web oficial del 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.

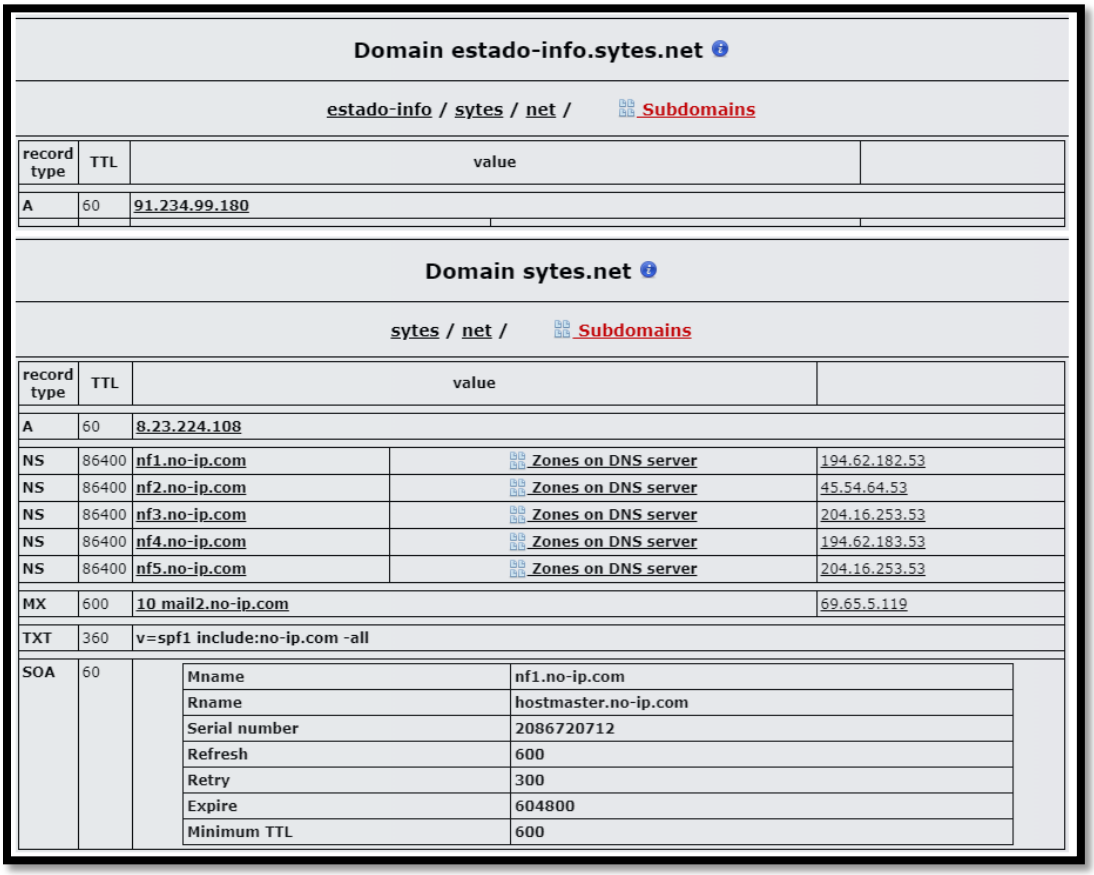
Indicadores de Compromisos

URLs

estado-info[.]sytes[.]net/portal/www[.]bancoestado[.]cl/

www[.]bancaaestada[.]info

www[.]bancaaestada[.]info/imagenes/comun2008/banca-en-linea-personas[.]php?html



Domain estado-info.sytes.net

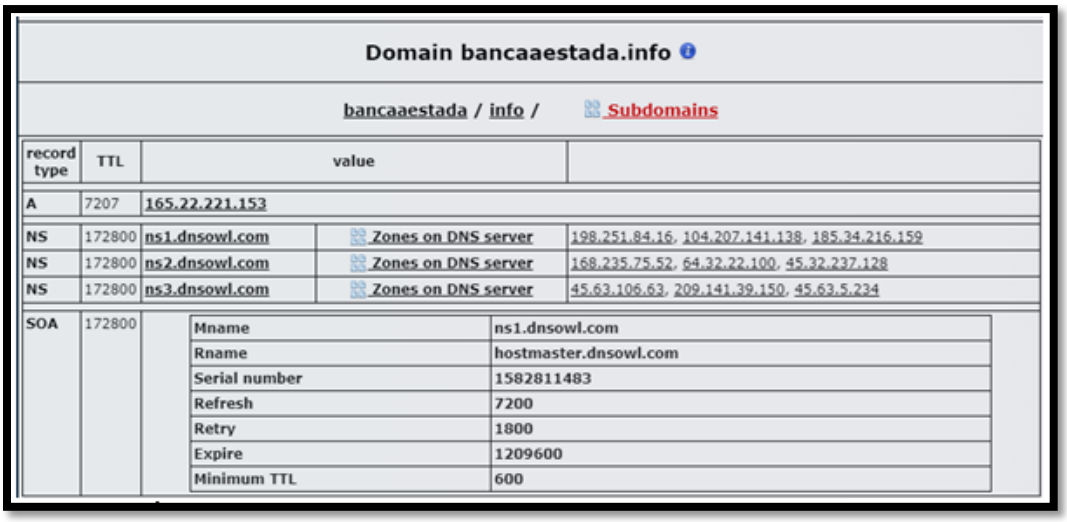
estado-info / sytes / net / Subdomains

record type	TTL	value
A	60	91.234.99.180

Domain sytes.net

sytes / net / Subdomains

record type	TTL	value		
A	60	8.23.224.108		
NS	86400	nf1.no-ip.com	Zones on DNS server	194.62.182.53
NS	86400	nf2.no-ip.com	Zones on DNS server	45.54.64.53
NS	86400	nf3.no-ip.com	Zones on DNS server	204.16.253.53
NS	86400	nf4.no-ip.com	Zones on DNS server	194.62.183.53
NS	86400	nf5.no-ip.com	Zones on DNS server	204.16.253.53
MX	600	10 mail2.no-ip.com		69.65.5.119
TXT	360	v=spf1 include:no-ip.com -all		
SOA	60	Mname	nf1.no-ip.com	
		Rname	hostmaster.no-ip.com	
		Serial number	2086720712	
		Refresh	600	
		Retry	300	
		Expire	604800	
		Minimum TTL	600	



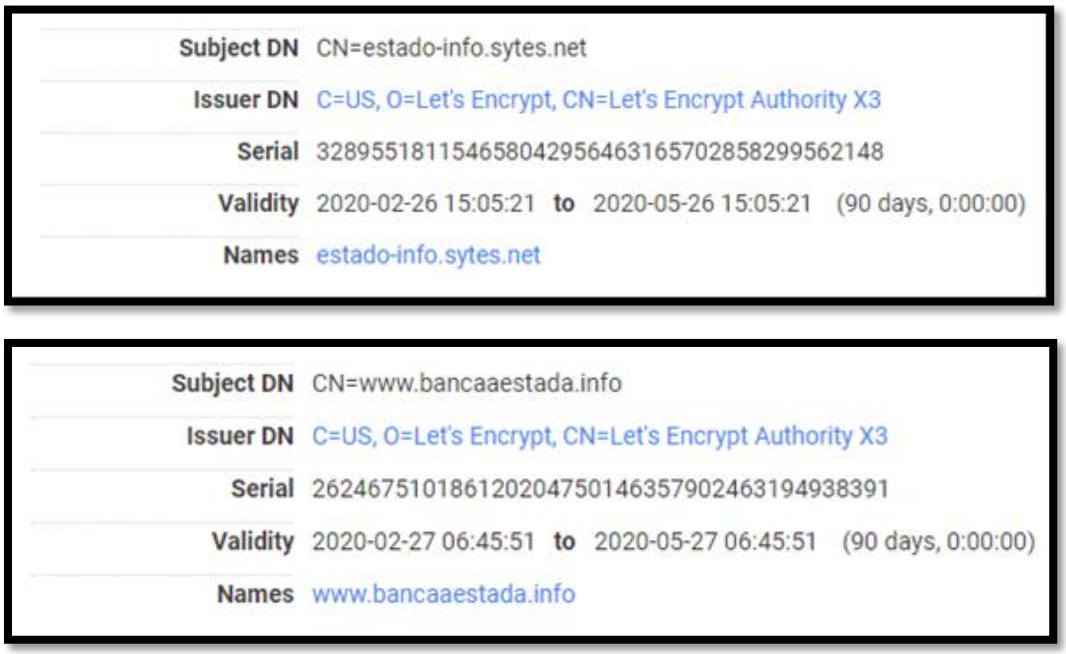
Domain bancaaestada.info

bancaaestada / info / Subdomains

record type	TTL	value		
A	7207	165.22.221.153		
NS	172800	ns1.dnsowl.com	Zones on DNS server	198.251.84.16, 104.207.141.138, 185.34.216.159
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	1582811483	
		Refresh	7200	
		Retry	1800	
		Expire	1209600	
		Minimum TTL	600	

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

Certificados



Subject DN	CN=estado-info.sytes.net
Issuer DN	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
Serial	328955181154658042956463165702858299562148
Validity	2020-02-26 15:05:21 to 2020-05-26 15:05:21 (90 days, 0:00:00)
Names	estado-info.sytes.net

Subject DN	CN=www.bancaaestada.info
Issuer DN	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
Serial	262467510186120204750146357902463194938391
Validity	2020-02-27 06:45:51 to 2020-05-27 06:45:51 (90 days, 0:00:00)
Names	www.bancaaestada.info

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

IP
91[.]234[.]99[.]180
165[.]22[.]221[.]153

Domain estado-info.sytes.net is located on IP address << 91.234.99.180 >>

Block start	91.234.99.0
End of block	91.234.99.255
Block size	256 Domains in block
Block name	PrivateInternetHosting
AS number	48666
Parent block	91.0.0.0 - 91.255.255.255
Organization	ORG-PIHL2-RIPE

Domain bancaaestada.info is located on IP address << 165.22.221.153 >>

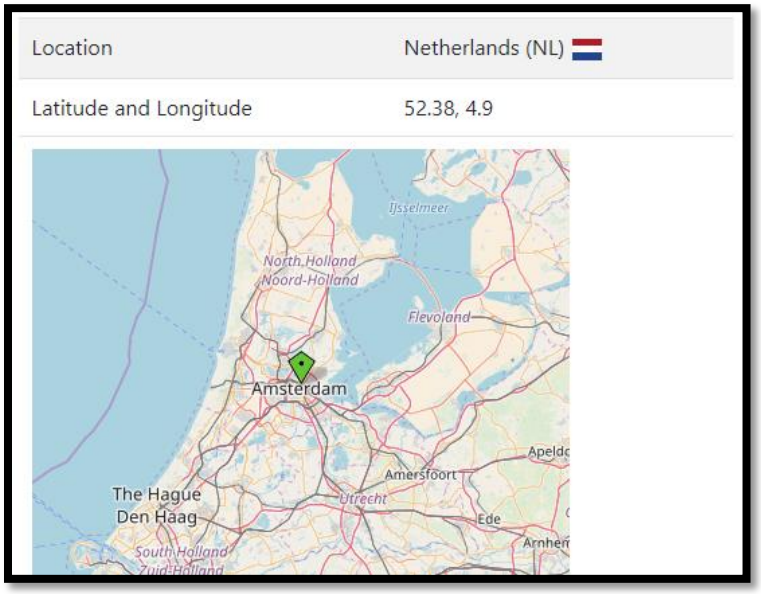
Block start	165.22.0.0
End of block	165.22.255.255
Block size	65536 Domains in block
Block name	CELTECH1
AS number	14061
Parent block	165.0.0.0 - 165.255.255.255
Organization	CellularTechnicalServices

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

Localización

Amsterdam, Noord-Holland, Netherlands

Bengaluru, Karnataka, India



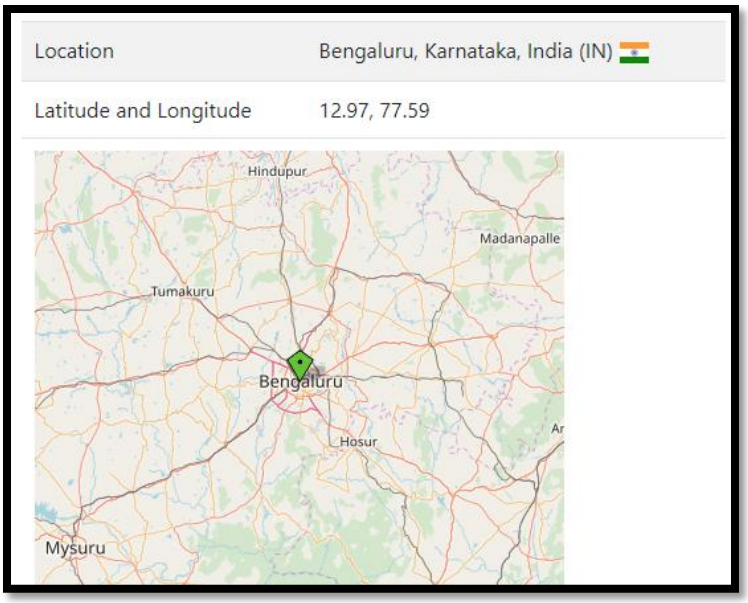
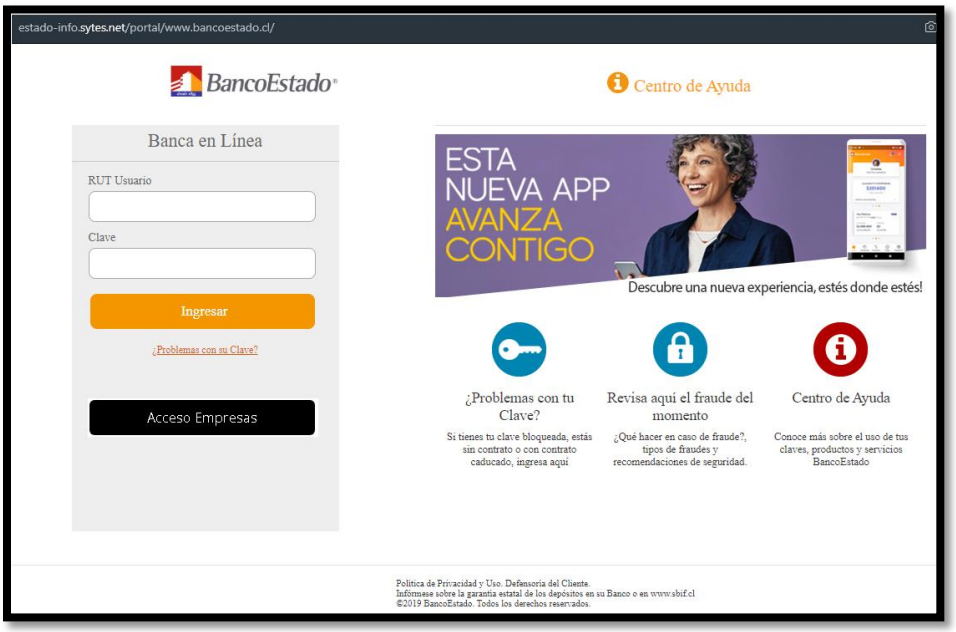
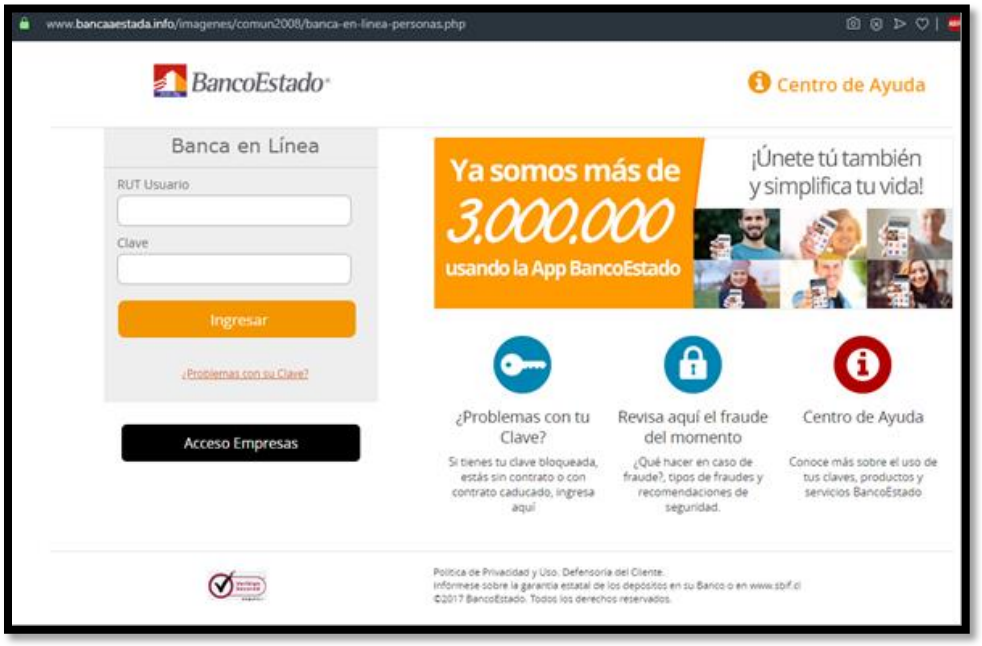


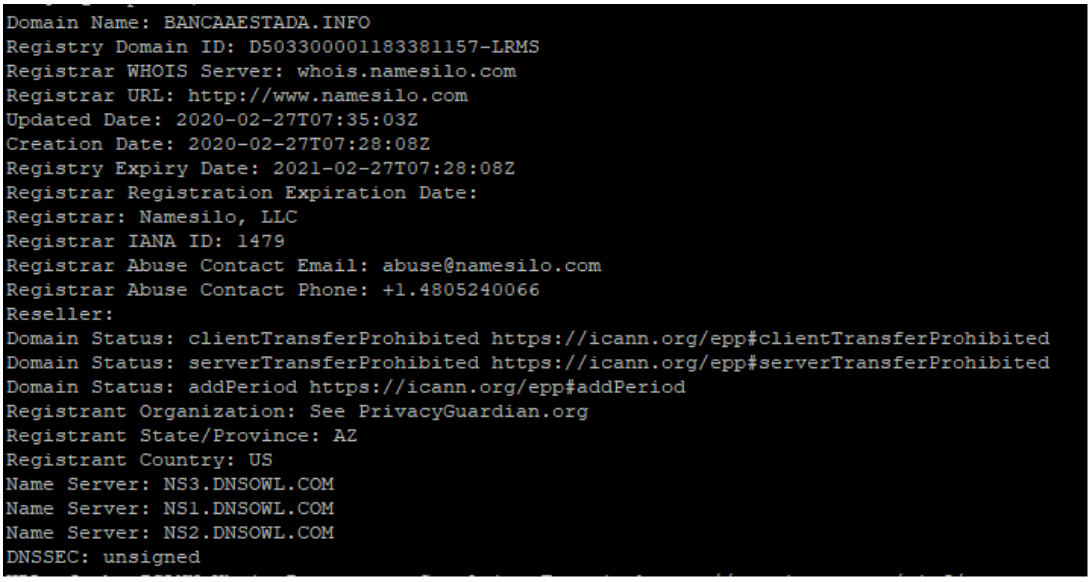
Imagen del sitio





Whois

```
Domain Name: sytes.net
Registry Domain ID: 5534045_DOMAIN_NET-VRSN
Registrar WHOIS Server: whois.srsplus.com
Registrar URL: http://srsplus.com
Updated Date: 2017-01-31T17:05:30Z
Creation Date: 1999-04-22T04:00:00Z
Registrar Registration Expiration Date: 2021-04-22T04:00:00Z
Registrar: TLDS LLC. d/b/a SRSPlus
Registrar IANA ID: 320
Reseller:
Domain Status: clientTransferProhibited http://icann.org/epp#clientTransferProhi
bited
Registry Registrant ID:
Registrant Name: Dan Durrer
Registrant Organization: No-IP.com
Registrant Street: 425 Maestro  Dr. Second Floor
Registrant City: Reno
Registrant State/Province: NV
Registrant Postal Code: 89511
Registrant Country: US
Registrant Phone: +1.7758531883
Registrant Phone Ext.:
Registrant Fax:
Registrant Fax Ext.:
Registrant Email: domains@no-ip.com
Registry Admin ID:
Admin Name: Dan Durrer
Admin Organization: No-IP.com
Admin Street: 425 Maestro  Dr. Second Floor
Admin City: Reno
Admin State/Province: NV
Admin Postal Code: 89511
Admin Country: US
Admin Phone: +1.7758531883
Admin Phone Ext.:
Admin Fax:
Admin Fax Ext.:
Admin Email: domains@no-ip.com
Registry Tech ID:
Tech Name: Dan Durrer
Tech Organization: No-IP.com
Tech Street: 425 Maestro  Dr. Second Floor
Tech City: Reno
Tech State/Province: NV
Tech Postal Code: 89511
Tech Country: US
Tech Phone: +1.7758531883
Tech Phone Ext.:
Tech Fax:
Tech Fax Ext.:
Tech Email: domains@no-ip.com
Name Server: nf3.no-ip.com
Name Server: nf2.no-ip.com
Name Server: nf4.no-ip.com
Name Server: nf1.no-ip.com
DNSSEC: Unsigned
```



```
Domain Name: BANCAAESTADA.INFO
Registry Domain ID: D503300001183381157-LRMS
Registrar WHOIS Server: whois.namesilo.com
Registrar URL: http://www.namesilo.com
Updated Date: 2020-02-27T07:35:03Z
Creation Date: 2020-02-27T07:28:08Z
Registry Expiry Date: 2021-02-27T07:28:08Z
Registrar Registration Expiration Date:
Registrar: Namesilo, LLC
Registrar IANA ID: 1479
Registrar Abuse Contact Email: abuse@namesilo.com
Registrar Abuse Contact Phone: +1.4805240066
Reseller:
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
Domain Status: addPeriod https://icann.org/epp#addPeriod
Registrant Organization: See PrivacyGuardian.org
Registrant State/Province: AZ
Registrant Country: US
Name Server: NS3.DNSOWL.COM
Name Server: NS1.DNSOWL.COM
Name Server: NS2.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: 2020.02.28 10:01:36 -03'00'