Alerta de seguridad cibernética	8FFR20-00319-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	07 de abril de 2020
Última revisión	07 de abril 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 un portal fraudulentos 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 COMPROMISO

URL
proceso-autenticacion-bestado-cl[.]dmeg[.]xyz

IP
3[.]16[.]128[.]111

DOMINIOS DONDE SE ALOJA URL

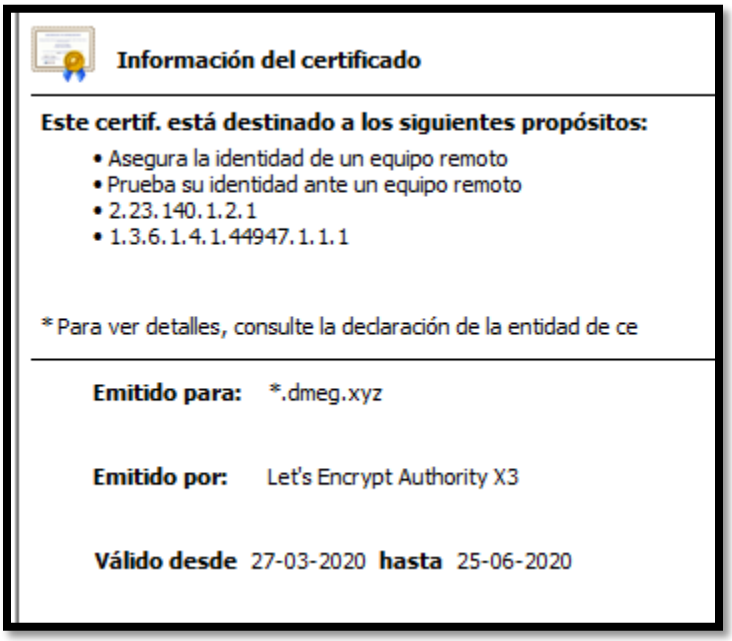
Domain dmeg.xyz

dmeg / xyz / Subdomains

record type	TTL	value		
A	300	3.16.128.111		
NS	300	ns1glr.name.com	Zones on DNS server	162.88.61.47
NS	300	ns2fhn.name.com	Zones on DNS server	162.88.60.47
NS	300	ns3jwx.name.com	Zones on DNS server	162.88.61.49
NS	300	ns4fpy.name.com	Zones on DNS server	163.114.217.49
SOA	3600			

Mname	ns1.name.com
Rname	hostmaster.nsone.net
Serial number	1585339745
Refresh	43200
Retry	7200
Expire	1209600
Minimum TTL	3600

CERTIFICADOS



Información del certificado

Este certif. está destinado a los siguientes propósitos:

- Asegura la identidad de un equipo remoto
- Prueba su identidad ante un equipo remoto
- 2.23.140.1.2.1
- 1.3.6.1.4.1.44947.1.1.1

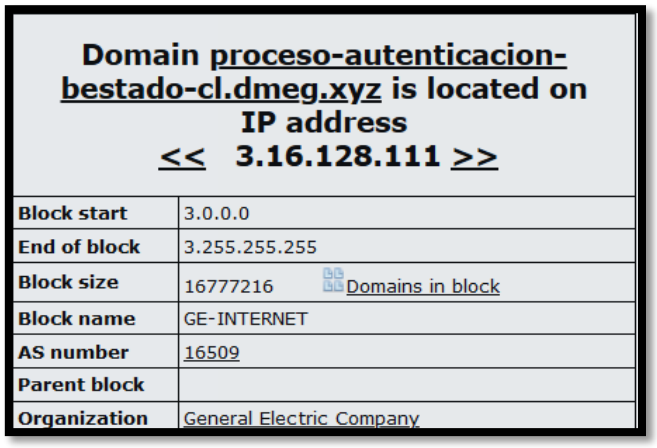
* Para ver detalles, consulte la declaración de la entidad de ce

Emitido para: *.dmeg.xyz

Emitido por: Let's Encrypt Authority X3

Válido desde 27-03-2020 **hasta** 25-06-2020

IP DE ORIGEN DONDE SE ALOJA SITIO



Domain proceso-autenticacion-bestado-cl.dmeg.xyz is located on IP address
<< 3.16.128.111 >>

Block start	3.0.0.0
End of block	3.255.255.255
Block size	16777216 Domains in block
Block name	GE-INTERNET
AS number	16509
Parent block	
Organization	General Electric Company

LOCALIZACIÓN

Columbus, Ohio, Estados Unidos

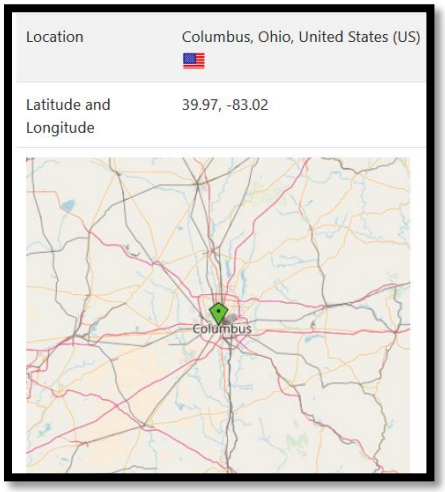
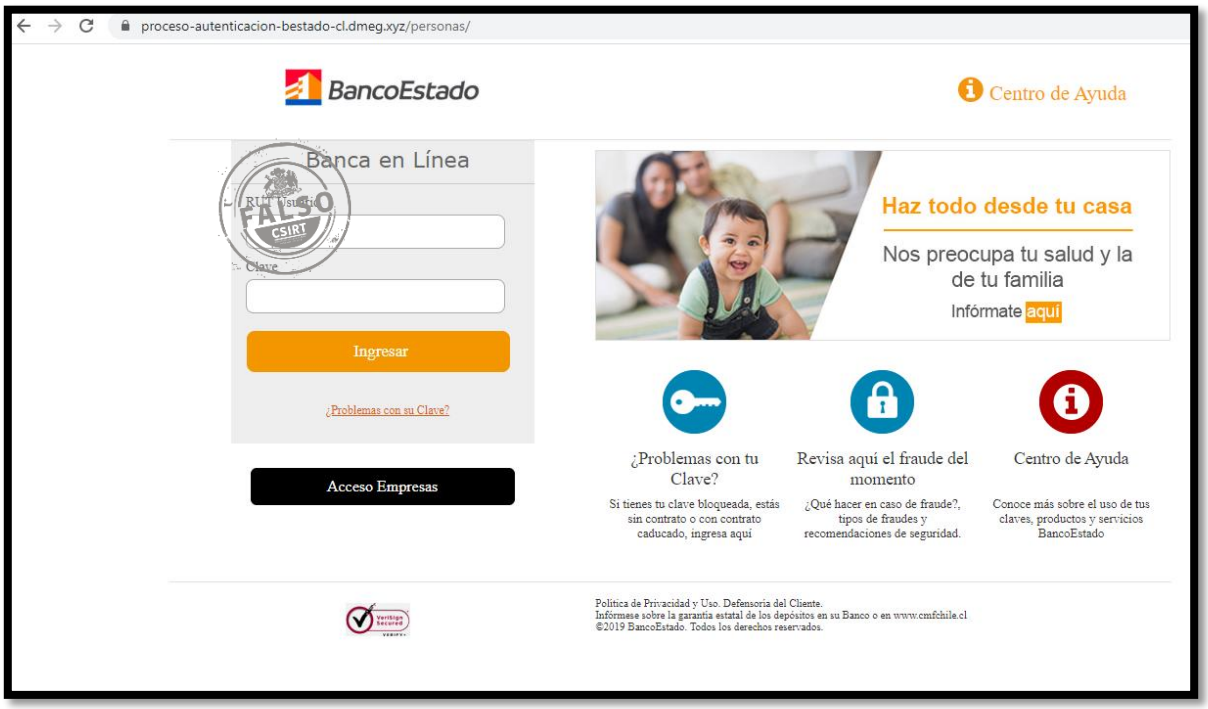


IMAGEN DEL SITIO



WHOIS

```
Domain Name: DMEG.XYZ
Registry Domain ID: D180211649-CNIC
Registrar WHOIS Server: whois.name.com
Registrar URL: http://www.name.com/
Updated Date: 2020-03-26T19:24:59.0Z
Creation Date: 2020-03-26T19:24:48.0Z
Registry Expiry Date: 2021-03-26T23:59:59.0Z
Registrar: Name.com LLC
Registrar IANA ID: 625
Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProh
ibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProh
ibited
Registrant Organization: Domain Protection Services, Inc.
Registrant State/Province: CO
Registrant Country: US
Registrant Email: Please query the RDDS service of the Registrar of Record ident
ified 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: NS1GLR.NAME.COM
Name Server: NS2FHN.NAME.COM
Name Server: NS3JWX.NAME.COM
Name Server: NS4FPY.NAME.COM
DNSSEC: unsigned
Billing Email: Please query the RDDS service of the Registrar of Record identifi
ed in this output for information on how to contact the Registrant, Admin, or Te
ch contact of the queried domain name.
Registrar Abuse Contact Email: abuse@name.com
Registrar Abuse Contact Phone: +1.4252982607
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of WHOIS database: 2020-04-06T21:50:44.0Z <<<
```

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: 2020.04.07 18:59:45 -04'00'