Centro Nacional de Seguridad Digital	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 129	Fecha: 13-05-2022
		Página 4 de 14

Componente que reporta	**CENTRO NACIONAL DE SEGURIDAD DIGITAL**		
Nombre de la alerta	Amenaza de suplantación de identidad a plataforma web GOB.PE		
Tipo de ataque	Suplantación	Abreviatura	Suplantación
Medios de propagación	Redes sociales, SMS, correo electrónico, videos de internet, entre otros		
Código de familia	G	Código de subfamilia	G03
Clasificación temática familia	Fraude		

Descripción

I. DATOS GENERALES:

El día 13/05/2022 se han identificado registros con intención evidente de suplantar la identidad de la plataforma GOB.PE.

II. EVIDENCIA:

- Se ha consultado por medio de protocolos de internet el uplink del dominio “gop[.]pe”

```
Domain Name: gop.pe
Sponsoring Registrar: 1API GmbH
Domain Status: ok
Registrant Name: Jurgen Neeme
Admin Name: Jurgen Neeme
Admin Street: Parnu Mnt 139C
Admin City: Tallinn
Admin State/Province: Harjumaa
Admin Postal Code: 11317
Admin Country: EE
Admin Email: jurgen@opus.ws
Name Server: ns1.parkingcrew.net
Name Server: ns2.parkingcrew.net
>>> Last update of WHOIS database: 2022-05-13T16:38:44.27Z <<<
```

- Se ha realizado el análisis con herramientas OSINT identificando múltiples registros apuntando a entidades del gobierno peruano.
- Según la fuente apunta a 87 registros e incluido un servicio de correo electrónico.

III. TEMA:

- La amenaza se oculta en los servicios de nube, las direcciones IP corresponden a los países de Canadá y Estados Unidos.

- La campaña de phishing por el momento parece estar en una etapa inicial, se ha confirmado en los registros las siguientes direcciones IP, se ha identificado un registro MX: mail[.]h-email[.]net

IP	PAÍS
104.247.82.52	CA, Canada
54.69.120.26	US, United States
34.221.92.59	US, United States
35.164.227.202	US, United States
54.214.124.53	US, United States
54.149.209.94	US, United States
54.218.19.107	US, United States
54.189.54.161	US, United States
54.212.151.52	US, United States
34.212.133.129	US, United States
52.38.197.157	US, United States

IV. CONCLUSIÓN:

- Toda persona natural o jurídica es libre de suscribir su nombre o marca en internet en los dominios .pe fácilmente por internet con las autoridades correspondientes.
- Sin embargo, “gop.pe” cuenta con una estructura de registros identificada que es alarmante.

V. RECOMENDACIÓN:

- Concientizar al equipo de trabajo en todos los niveles de la institución.
- Contar con directrices vigentes de autenticación multifactor en los sistemas de información.
- Contar con soluciones de ciberseguridad vigentes y actualizadas.
- Contar con un plan de respuesta ante incidentes.

Fuentes de información	▪ Análisis propio y de fuentes OSINT