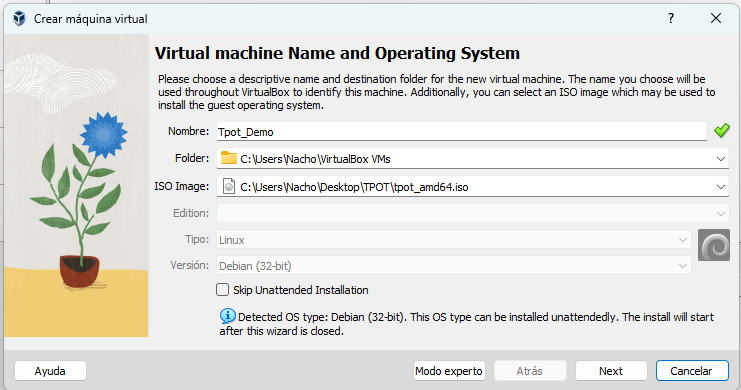
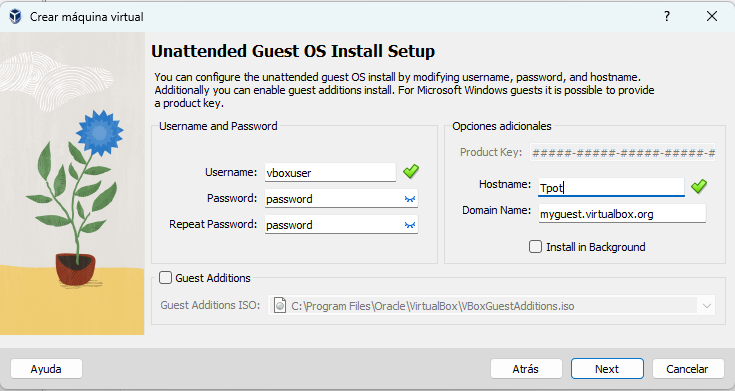
Vamos a realizar la instalación de cero:

En primer lugar, creamos la máquina virtual:

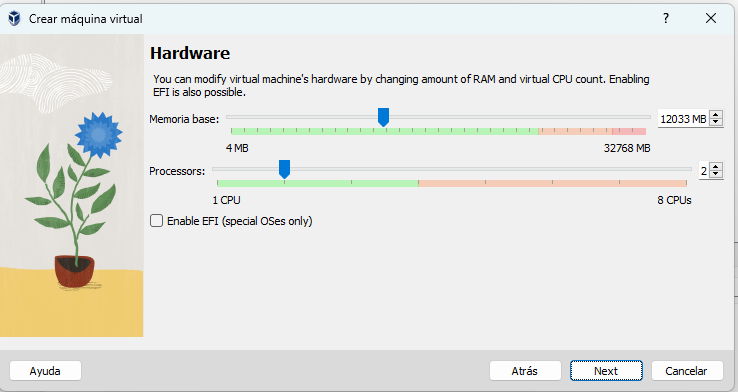


Ojo, lo detenta como un sistema de 32 bits. Mejor no darle la imagen o cambiarlo luego.

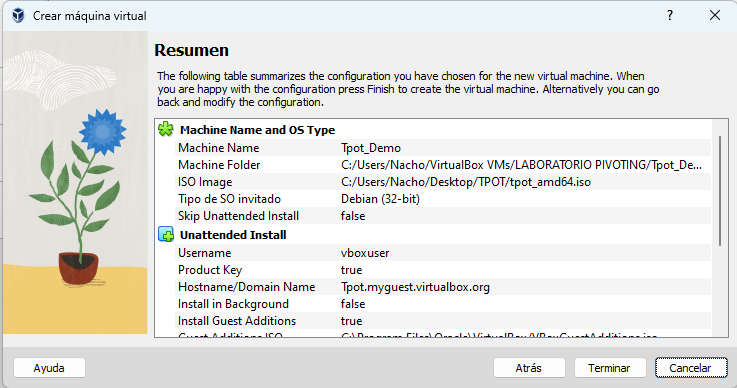
Fijamos los valores que nos pide:



Asignamos los recursos necesarios. En nuestro caso, 12GB y dos núcleos.



Y finalizamos la instalación.



Usuario del Host: tsec/demos

Web: nacho/demos

La imagen que bajamos es una imagen ligera, que luego se descarga el sistema operativo. Contiene una instalación desatendida de Debian. Sobre esa, instala lo necesario para el HoneyPot.

Una vez instalado, disponemos de las siguientes conexiones:

una consola de administración,

un servicio SSH

dos webs para administración del sistema y gestión del honeypot.

En cuanto a los interface de red, nos deja un eth0, para la gestión, levantando múltiples interfaces de red para el resto de las máquinas y servicios.

Web de administración:

<https://192.168.1.18:64294/>

Web de gestión:

<https://192.168.1.18:64297/>

SSH:

ssh://192.168.1.18:64294/64295

En la primera instalación tenemos errores con el servicio de red, el adaltador enp0s3 y con la web de gestión.

Creamos la máquina de nuevo, con mas disco y no thin provisioning.

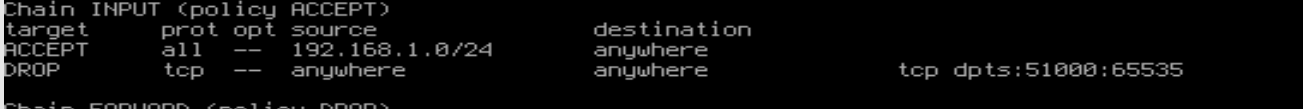
Configuramos la dmz y limitamos los puertos expuestos hasta el 50000.



Bloqueamos las conexiones entrantes de gestión

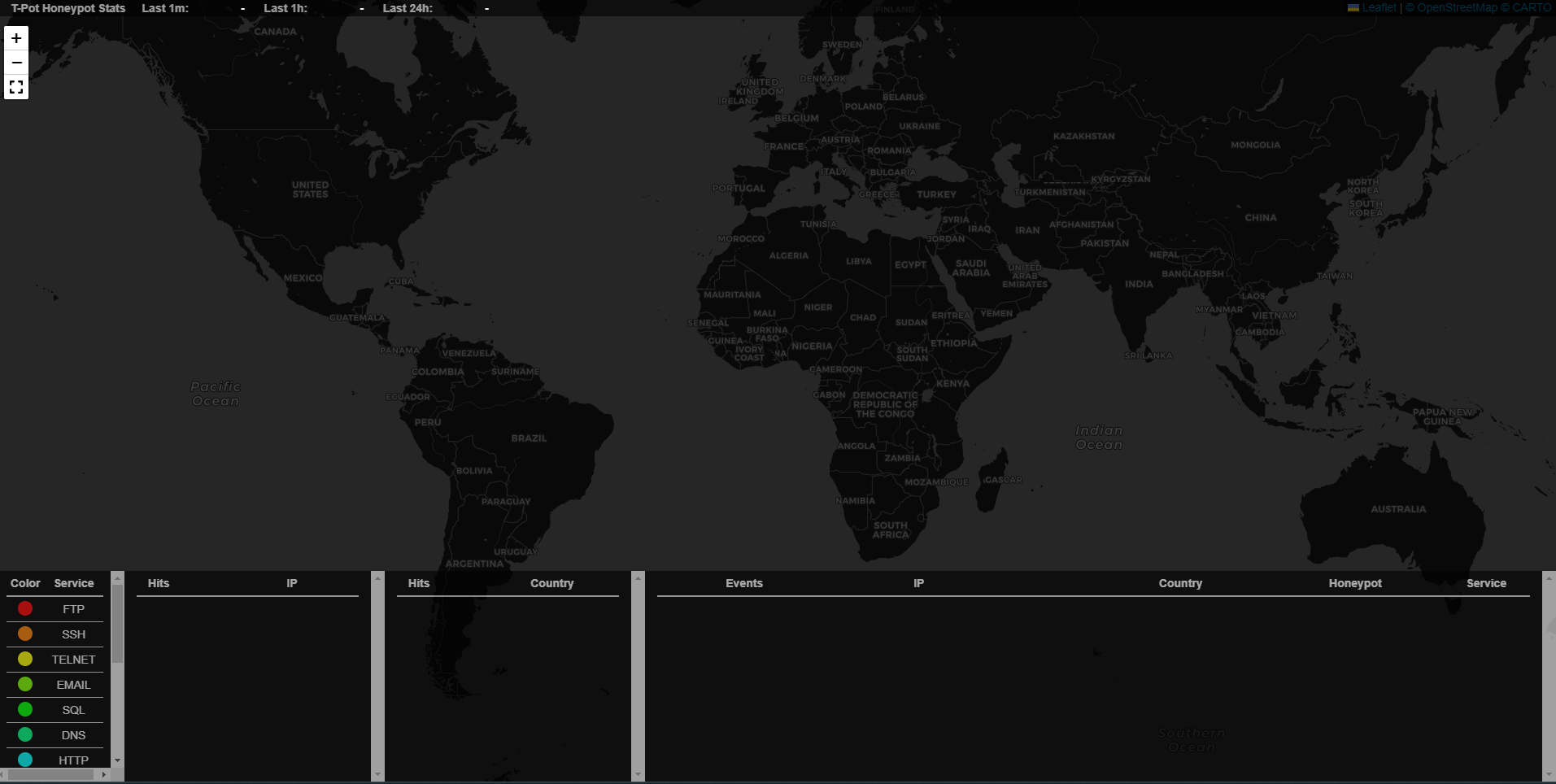
sudo iptables -I INPUT -s 192.168.1.0/24 -p ip -j ACCEPT

sudo iptables -A INPUT -s 0.0.0.0 -p tcp --dport 50000:65535 -j DROP



Y empezamos.

Primera conexión a Internet, 10/5/2023, 9:23 horas. (Abrimos puertos ftp, ssh, 445, etc…)

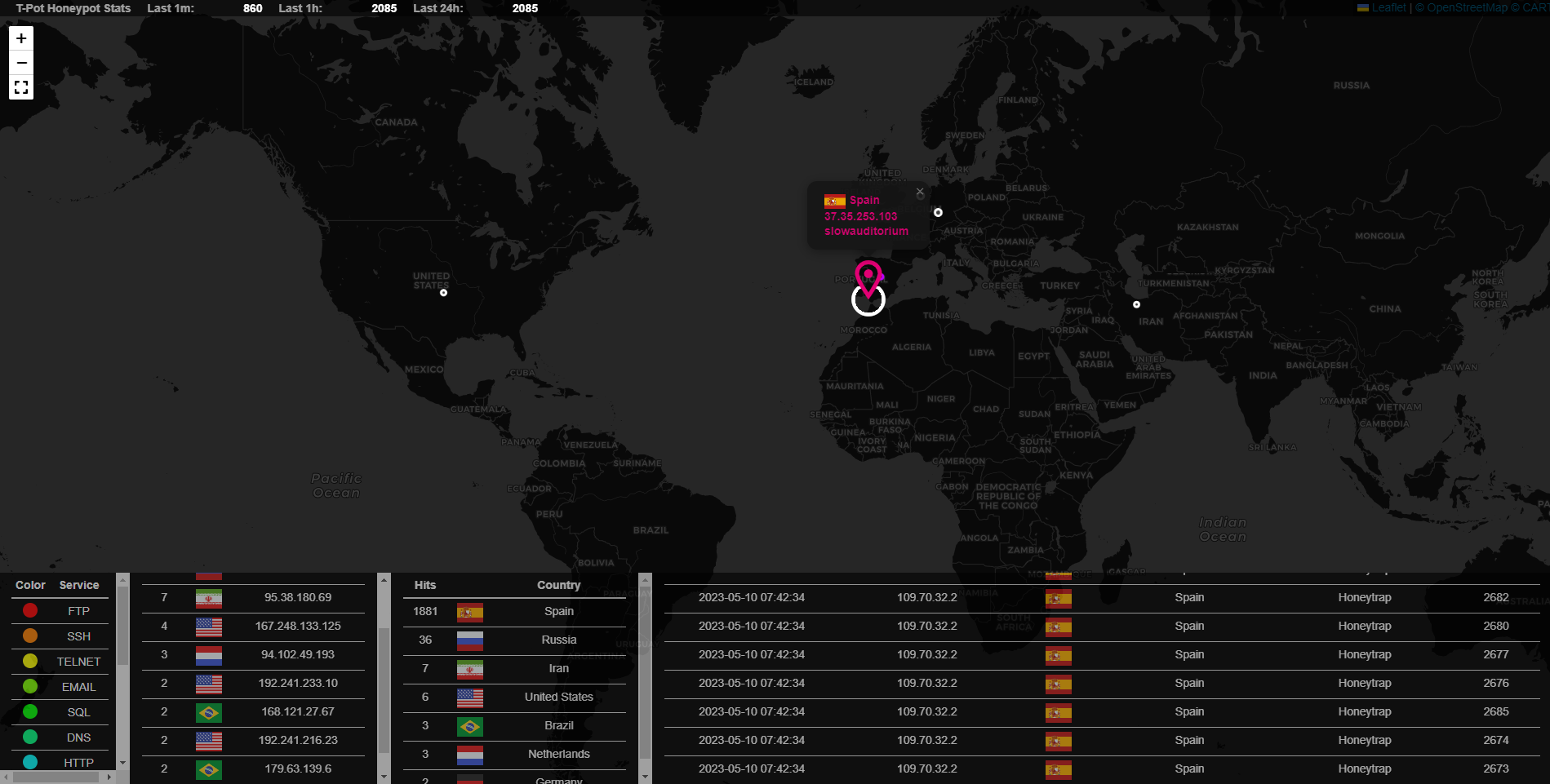


Comprobamos la visibilidad de los puertos desde Internet:

Cuando comenzamos con el escaneo de puertos desde la web:

<https://www.testdevelocidad.es/test-de-puertos/>





Vemos que el honey pot que está detectando ahora es honeytrap.

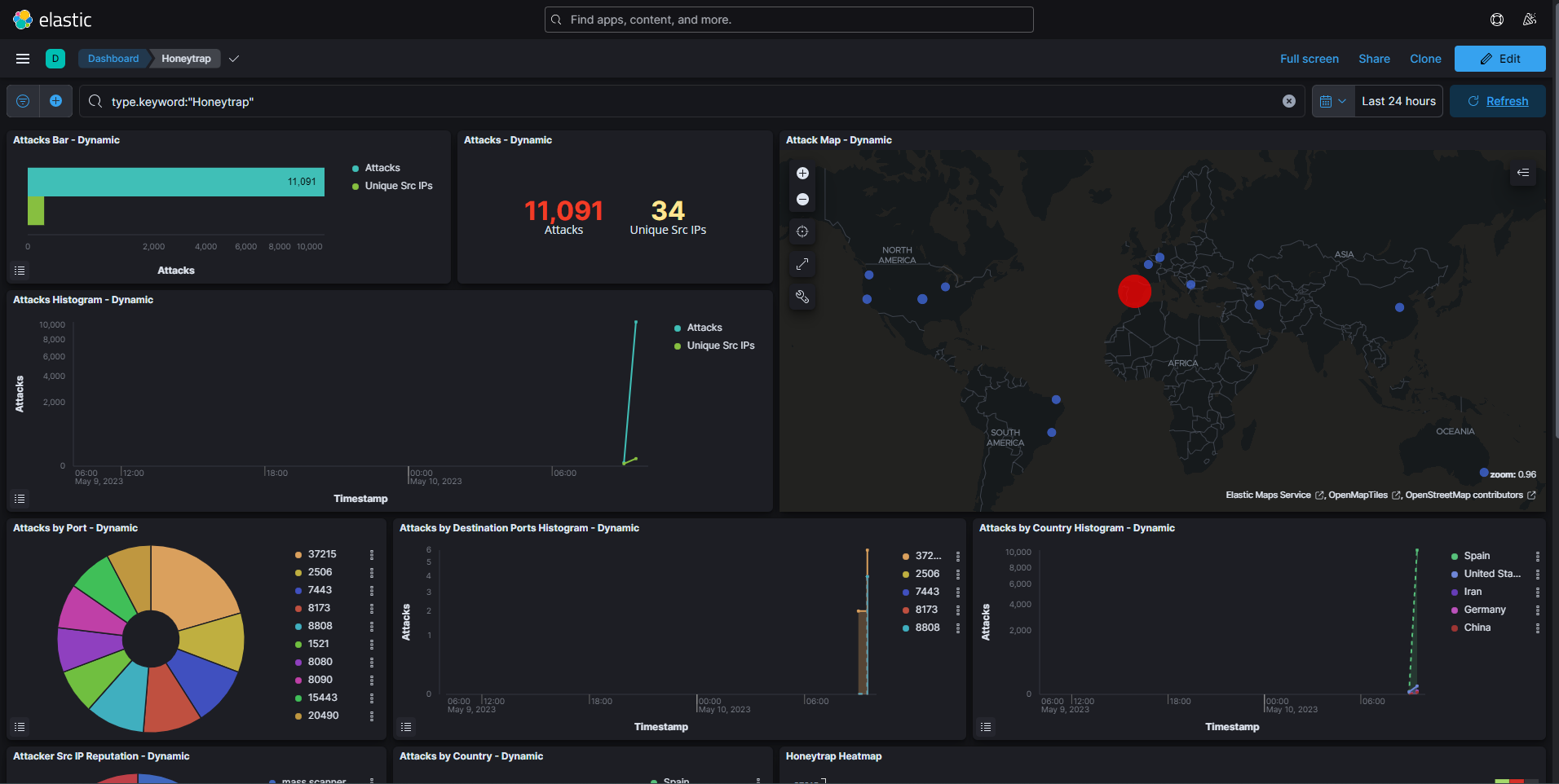
Podemos pensar que estas conexiones se refieren a las conexiones del escaneo de puertos…

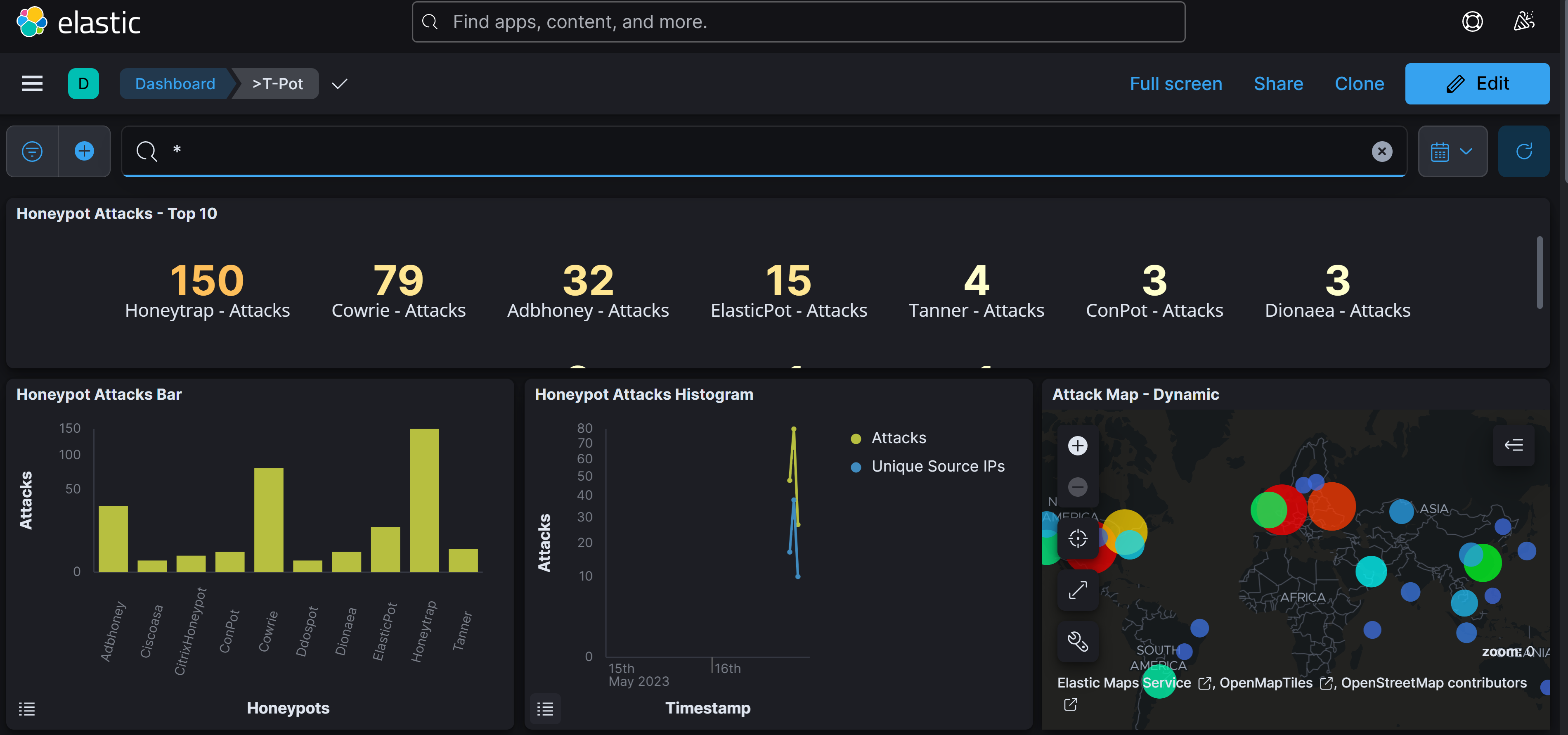
Pero si observamos, vemos distintas IP’s…

Vamos a ver su cuadro de mando: KIBANA

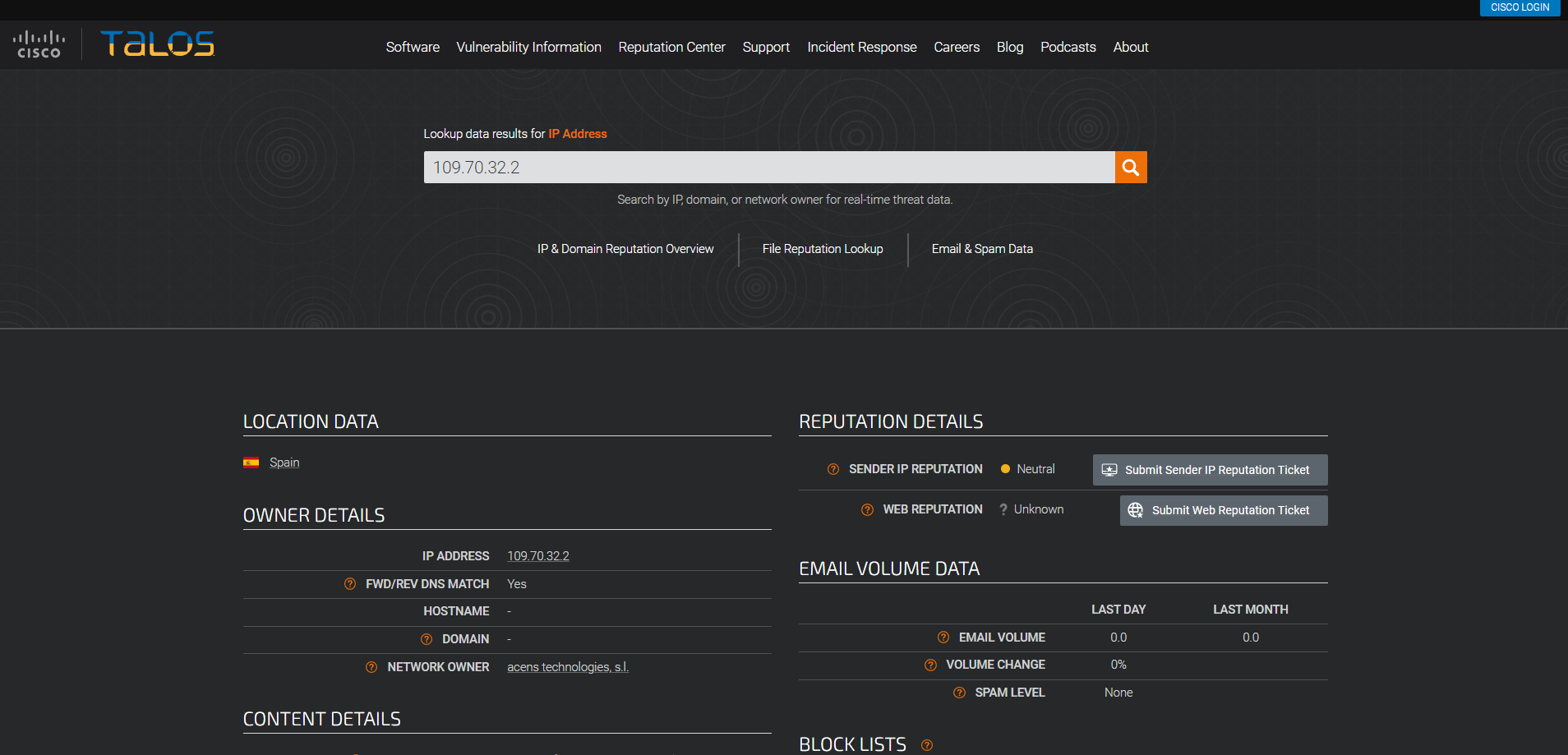
Para arrancar Kibana debemos hacer una pequeña modificación en el fichero de configuración de elasticsearch, elasticsearch.yml, que se nos indica al conectarnos al Elasticvue. Para esto lo mejor es conectarnos con un cliente SSH.

Aquí podemos ver distintos indicadores para cada HP, pero hay un cuadro de mando (dashboard) especialmente diseñado que nos permite explorar todas las opciones, T-POT.



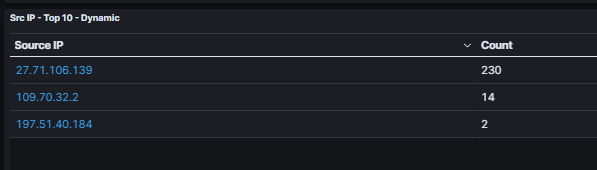


Desde la lista de IP’s que aparecen al final, podemos visualizar el resultado de reputación:



Vemos la reputación de la Ip que ataca desde Vietnam:

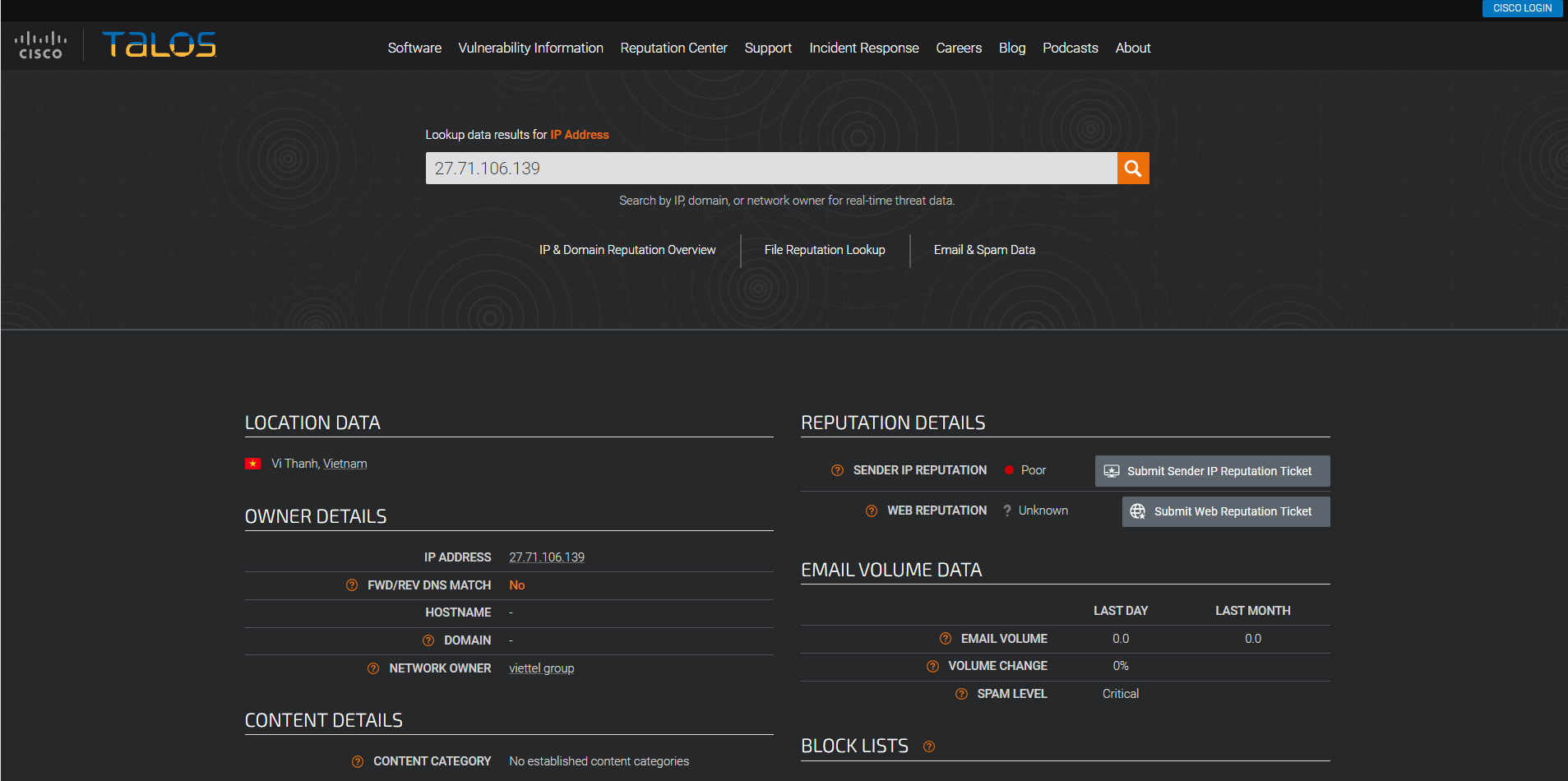




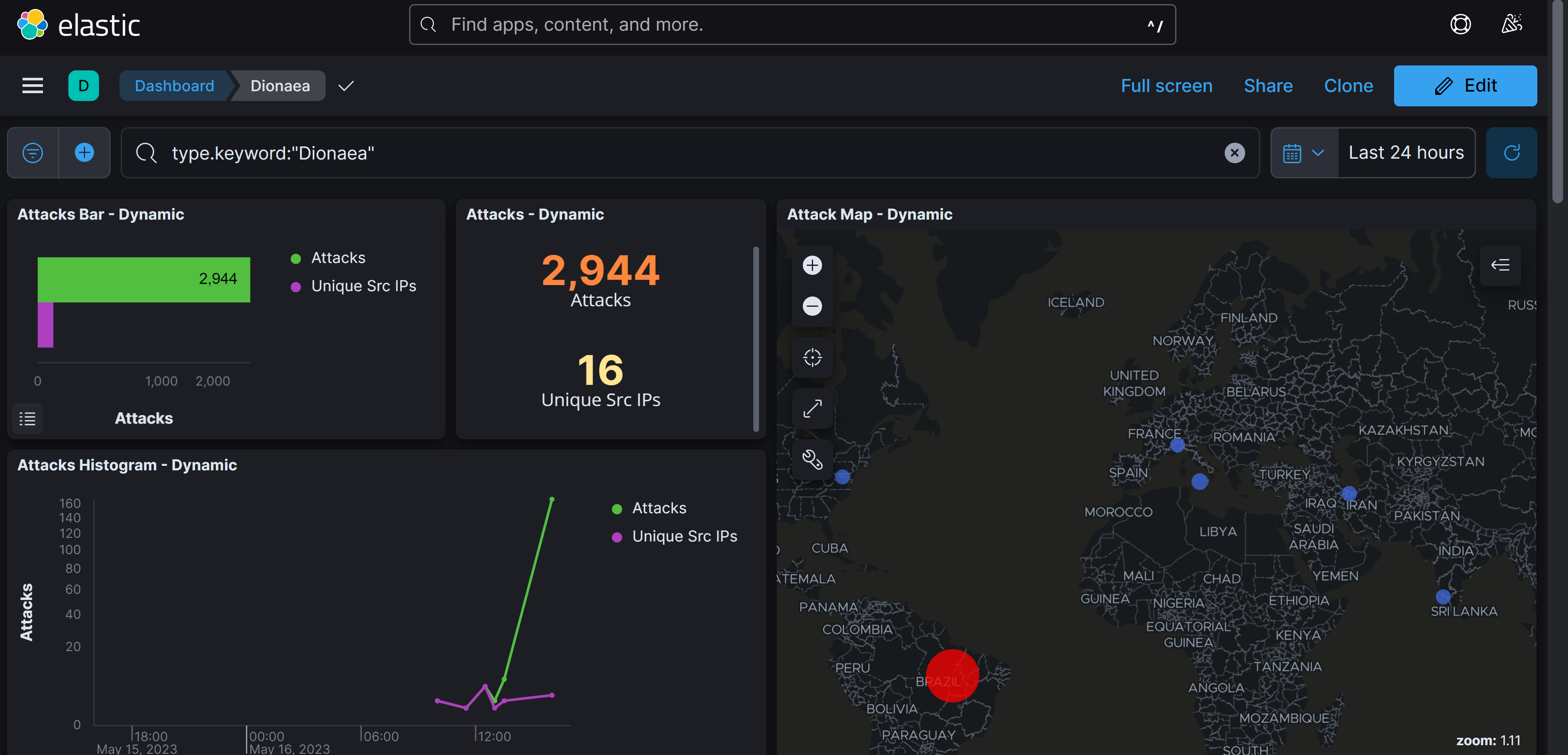
Es interesante explorar los datos que nos ofrece sobre cada honeypot. En concreto, de Cowrie, podemos ver los comandos ejecutados desde su panel de Kibana:



También los ficheros descargados y urls solicitadas.



Ver el plugin de Dianonea y los ataques a 445.



En T-pot y por puerto 445, podemos encontrar las firmas de Suricata.

Por último, podemos explorar el directorio de /data/dianoea/binaries…

Ponemos sudo python -m SimpleHTTPServer 65533 y nos lo traemos con Firefox, y a virustotal.

<https://pythones.net/crear-servidor-python-http/>

Comandos interesantes:

/opt/tpot/bin/dps.sh

Systemctl status tpot.service

* Nos faltaría disponer de algún vídeo de cómo se muestran los ataques.
* Realizar ataques internos.
* Obtener datos de comandos ejecutados o exploits, para intentarlo desde Kali en el mismo entorno.
* ¿Qué ve el atacante?? Estaría bien desde esta perspectiva, ver que ve el atacante.

URLS de interés:

<https://github.com/telekom-security/tpotce/#technical-concept>

Fuente dianoea interesante:

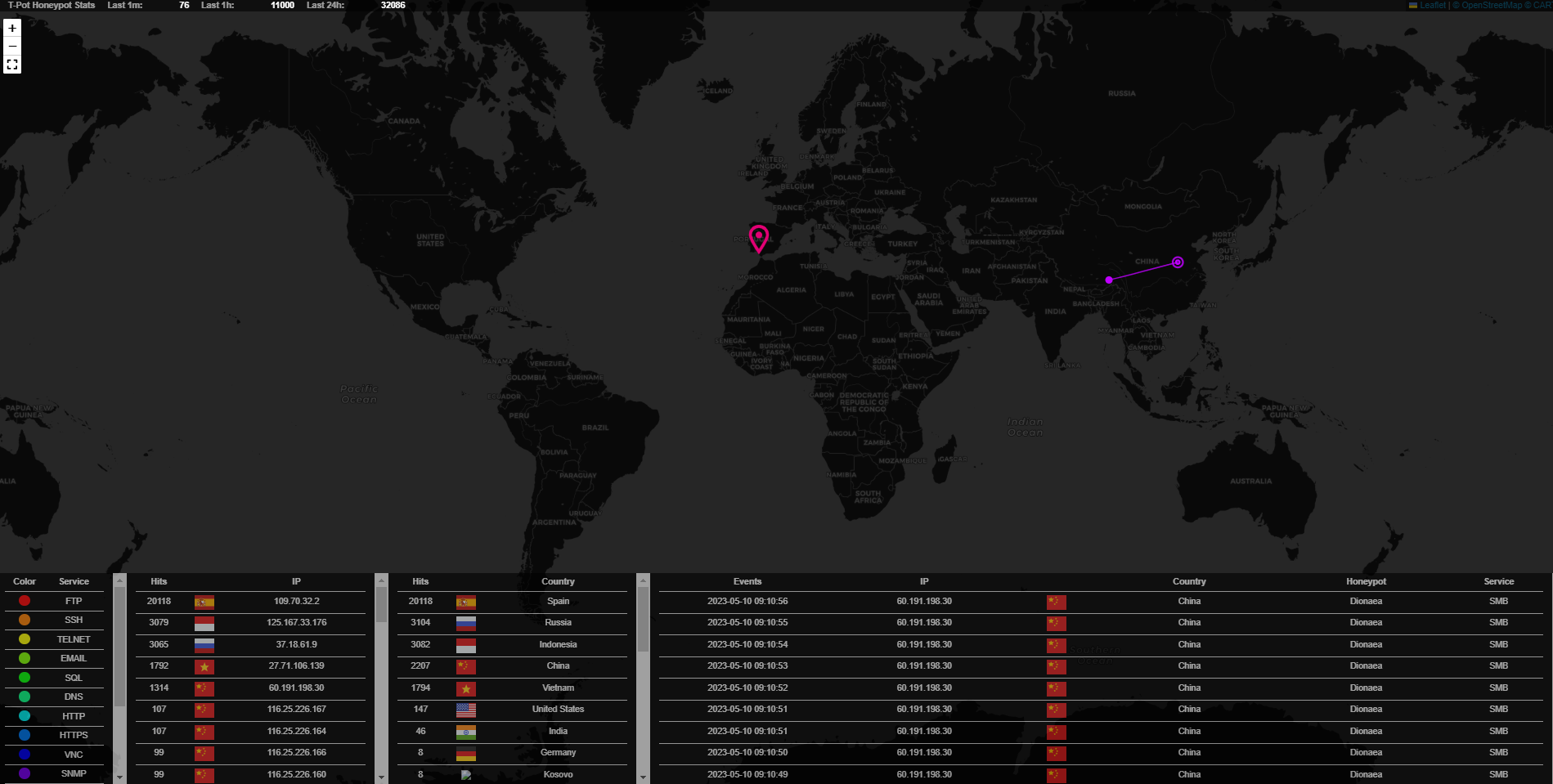
<https://revista.seguridad.unam.mx/numero23/poc-captura-de-malware-con-el-honeypot-dionaea-parte-i>

Instalación:

<https://blog.elhacker.net/2021/01/instalar-honeypot-t-pot-en-una-maquina-virtual-tpotce-cowrie-docker-dionea.html>

Se van incorporando nuevos actores a la fiesta.

Observar los colores de los ataques,q ue se corresponden con los distintos servicios:



Ver securityMeter, enlace externo dónde vemos en TR los ataques a dispotivos T-Pôt

<https://www.sicherheitstacho.eu/start/main>