**Actividades Tema 1**



Daniel Escaño Hernández CET Ciberseguridad

# 

# **1. Índice:**

[**1. Índice:**](#_4jq84lualx9d) **1**

[**2. Actividades**](#_ofiic1av8ddq) **2**

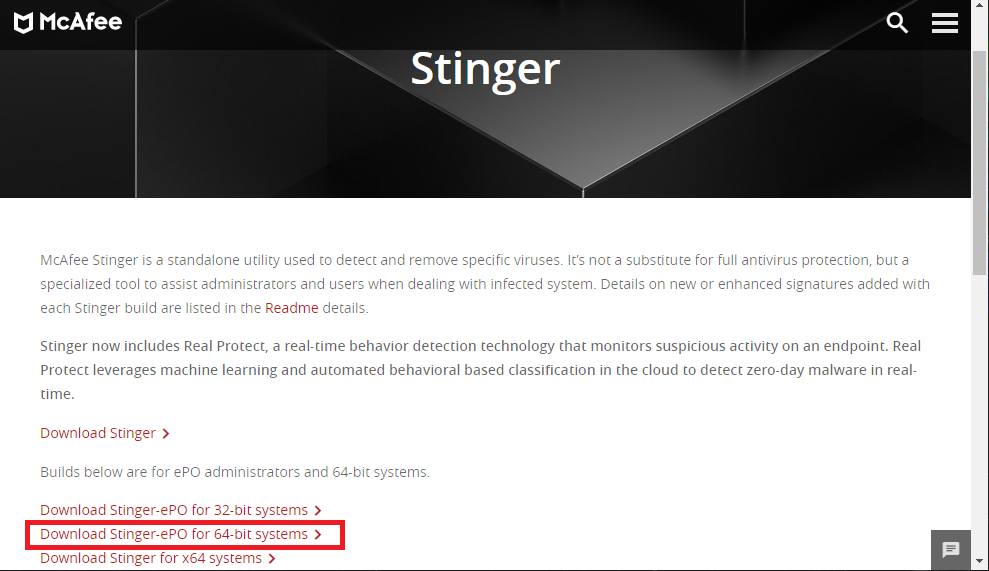
[**2.1 Actividad 1.6.1**](#_5d38uxjyswtl) **2**

[**2.2 Actividad 1.6.2**](#_kuhsn9136ml3) **5**

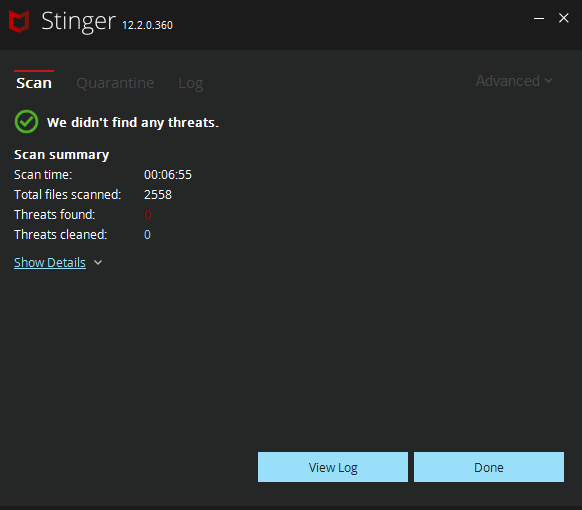
# **2. Actividades**

### **2.1 Actividad 1.6.1**

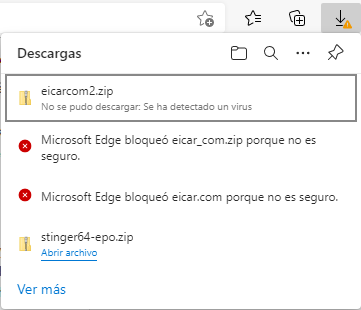
Descargamos el software a utilizar, en este caso: McAfee, en concreto Stinger.



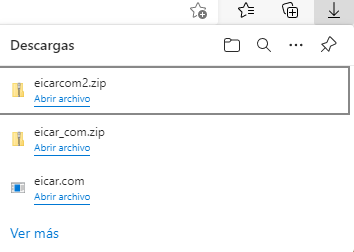
Realizamos un primer escáner para comprobar el funcionamiento del software y para comprobar los cambios ejecutados a lo largo del ejercicio.



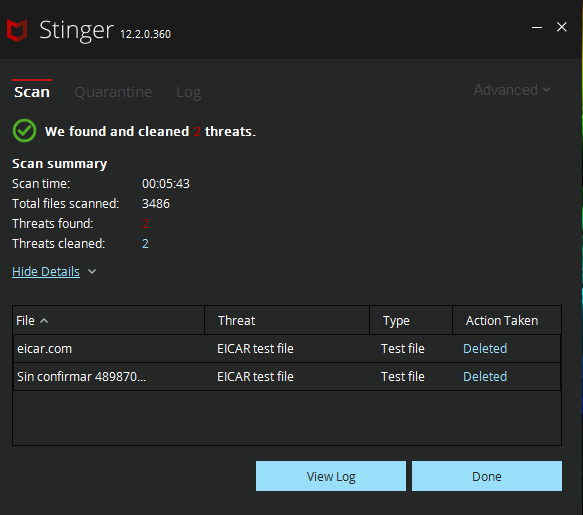
Procedemos a la descarga de malware desde la página de Eicar, no saltaran errores de descarga debido a la configuración actual de nuestro navegador además de nuestro sistema Firewall



Desactivamos el Firewall, las medidas de seguridad del sistema operativo y navegador. Y procedemos a la descarga, observaremos como ahora sí nos permite guardar el archivo en nuestro equipo.



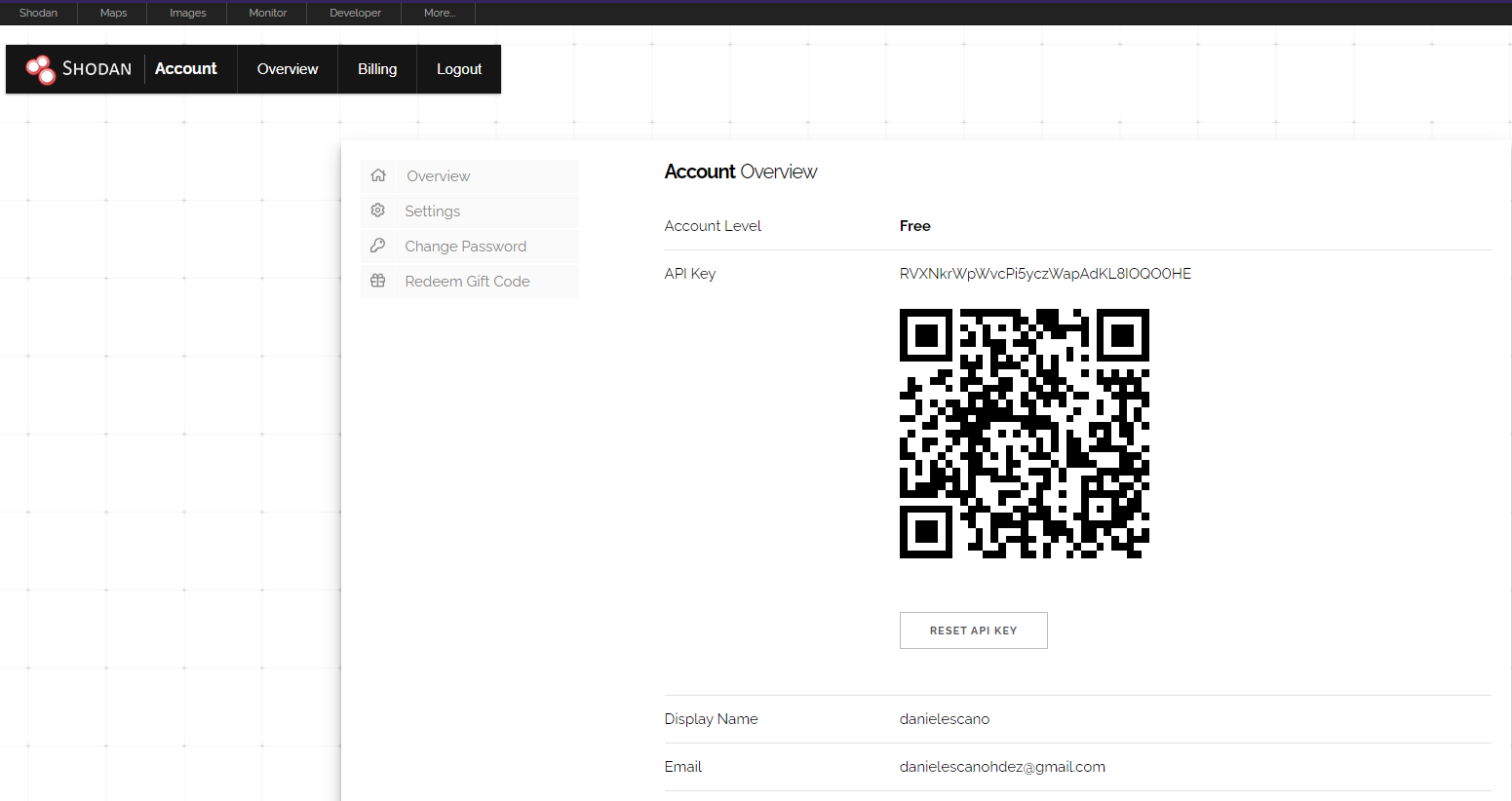
Nuevamente realizamos un examen para comprobar que el software funciona correctamente y nos alerta de las amenazas en nuestro sistema de ficheros



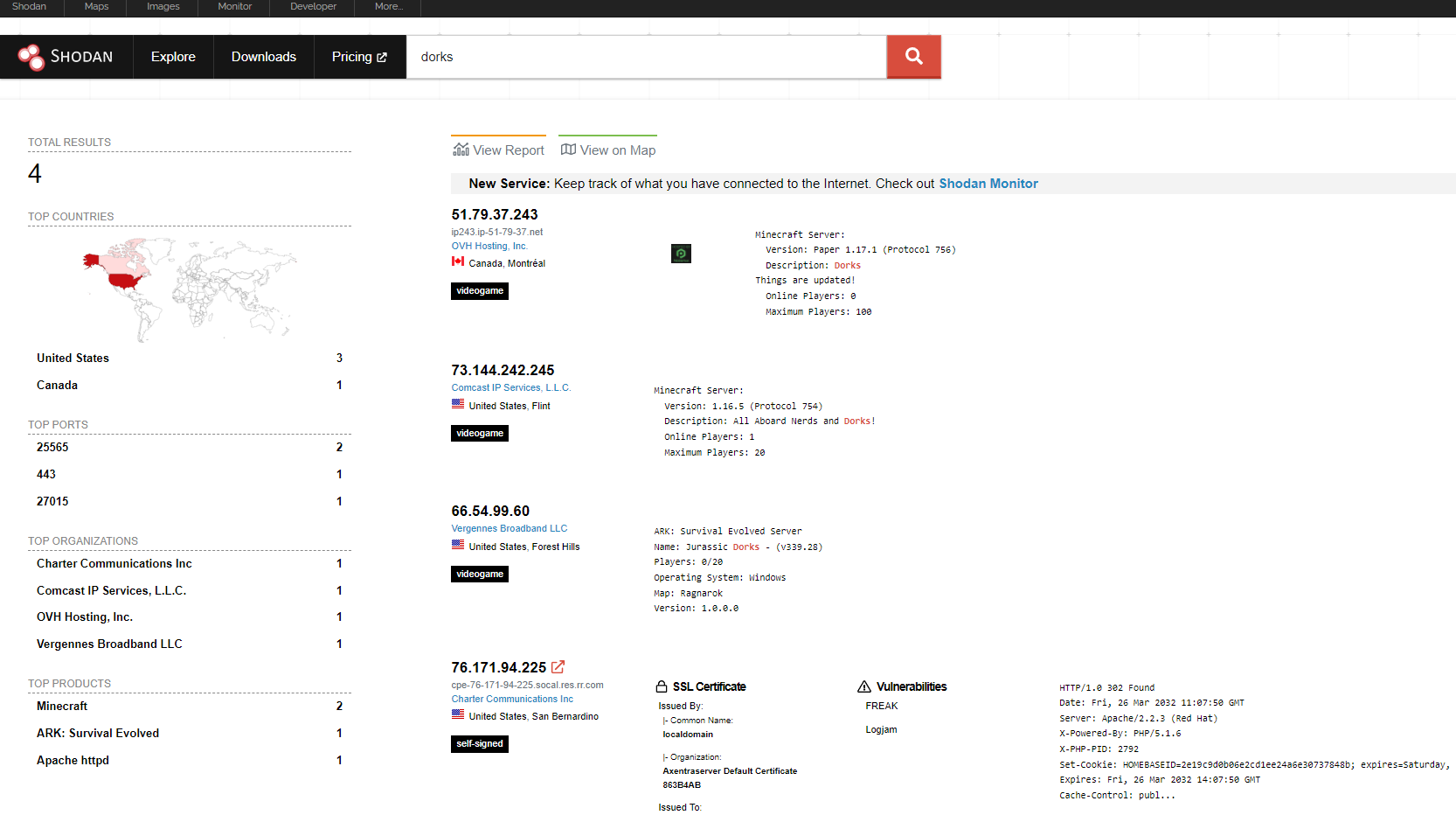
### **2.2 Actividad 1.6.2**

Utilizaremos para esta actividad shodan.io, un motor de búsqueda de vulnerabilidades en

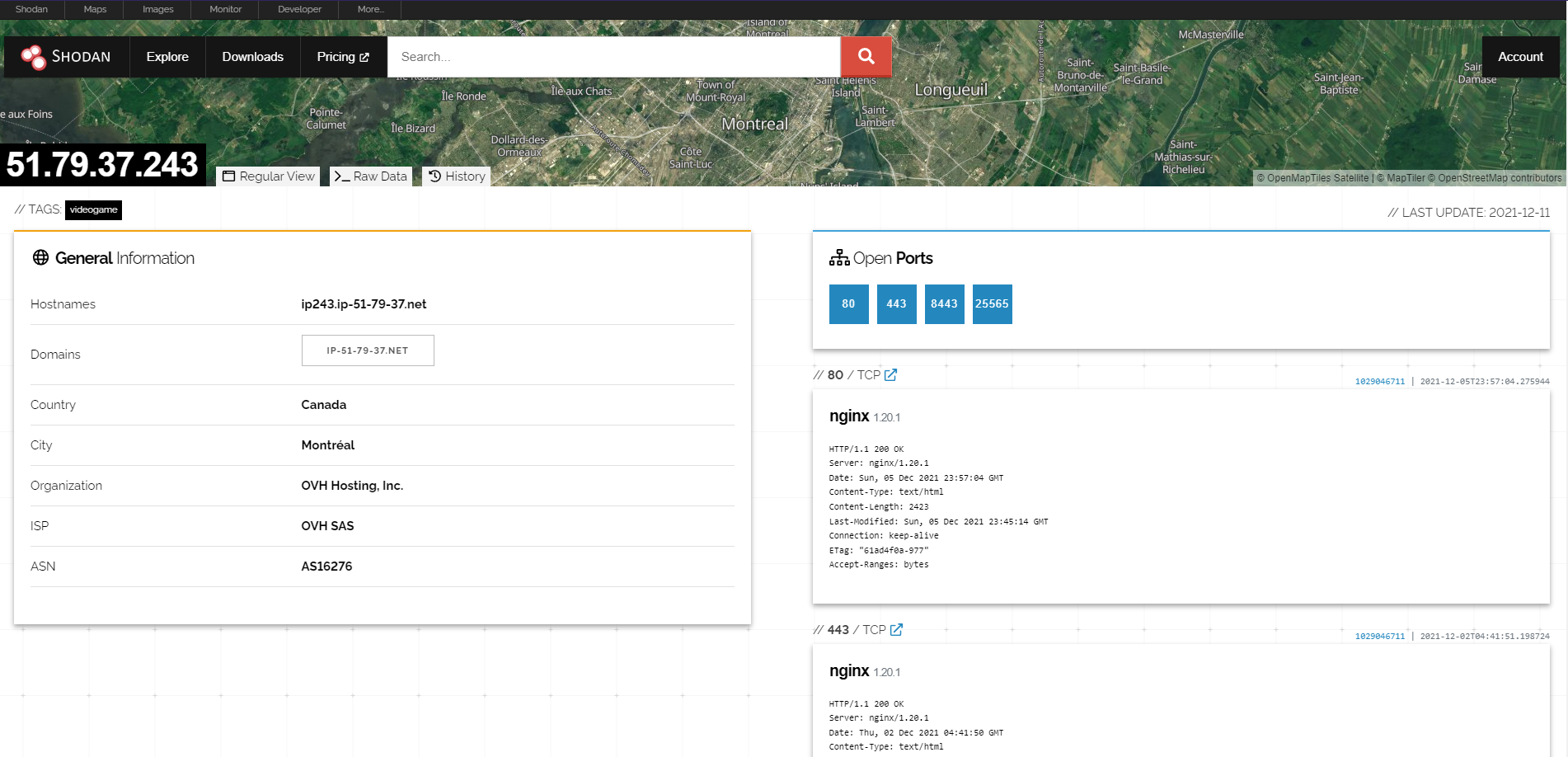
sistemas localizados en todo el mundo, lo primero que necesitamos es registrar una cuenta.



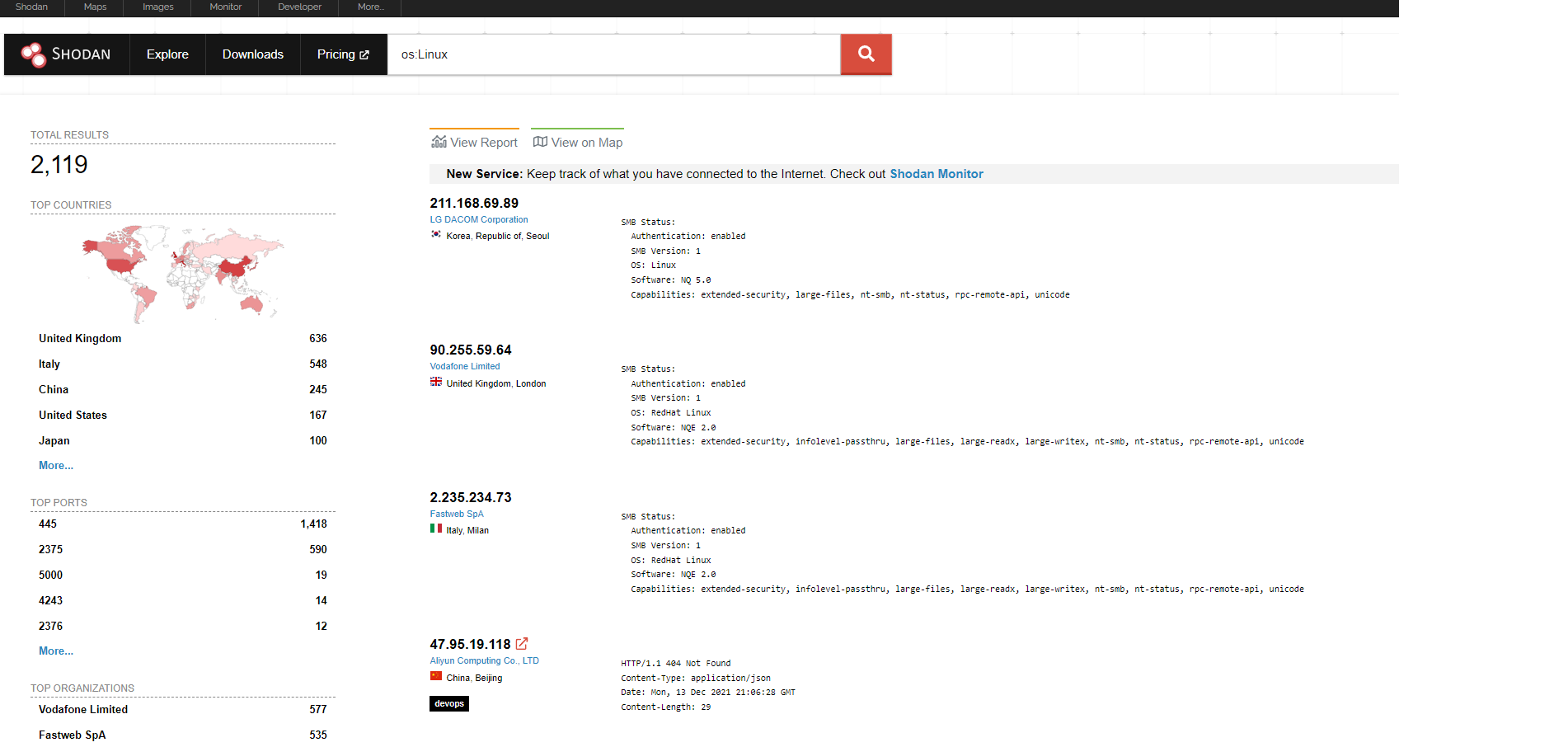
Una vez creada la cuenta podemos proceder a realizar diferentes búsquedas con filtros específicos que nos puedan interesar. A continuación varios ejemplos:



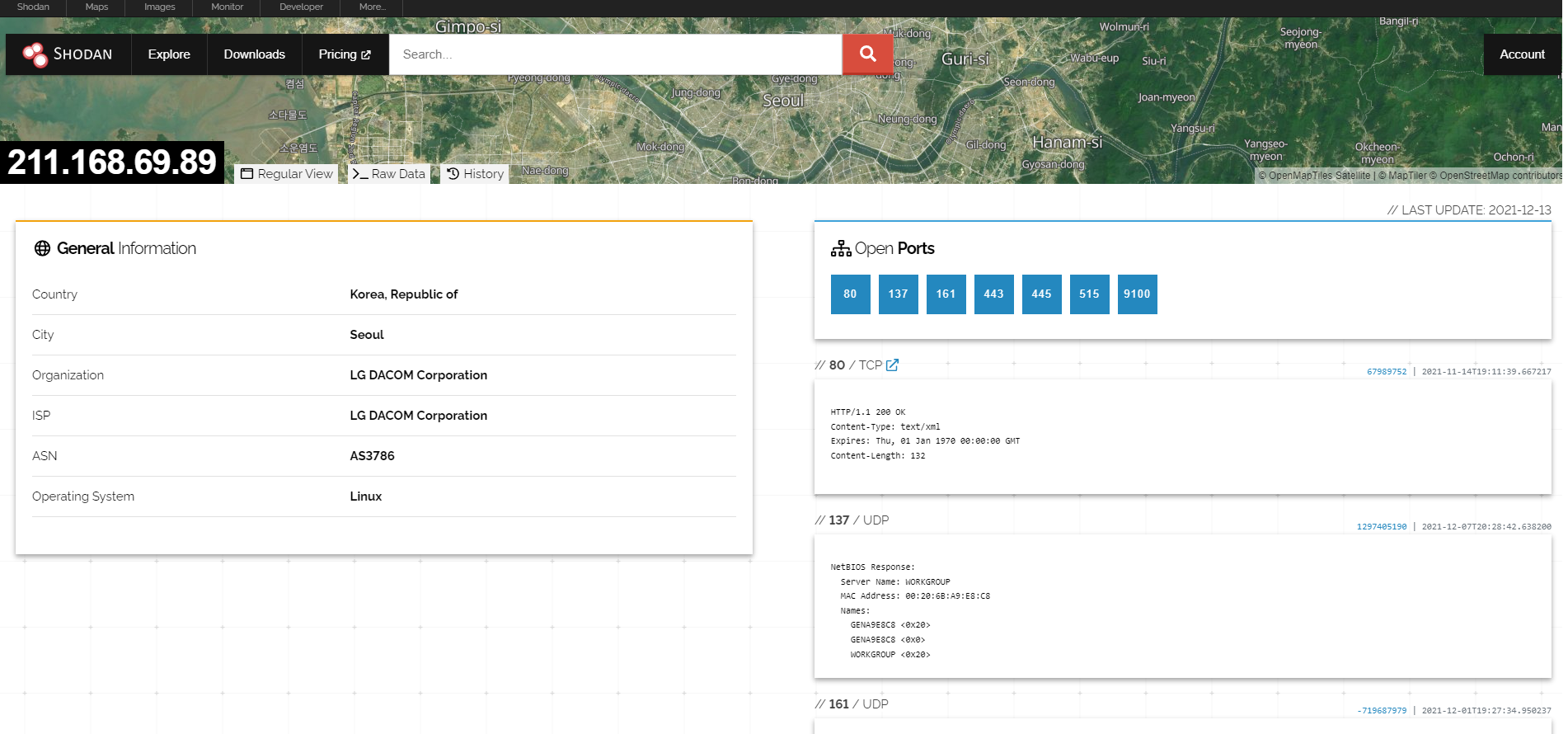
Podemos observar la información de forma detallada en cada caso.



En este caso el parámetro de búsqueda añadido es: “os:Linux”, mostrándonos todos los equipos con sistema operativo Linux que poseen una vulnerabilidad y están registrados en shodan.io



Una vez más podemos observar con detalle cualquiera de los casos encontrados.



Esta última búsqueda es realizada con el parámetro: “country:es”. Dándonos como resultado todos los sistemas informáticos con vulnerabilidades detectados en el territorio Español.

