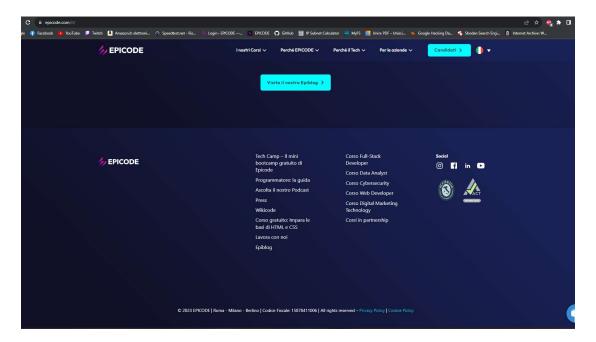
Esercitazione raccolta informazioni

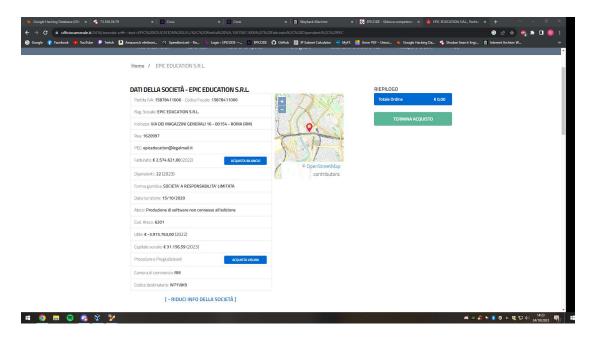
Target: Epicode

Durante questo esercizio andremo a raccogliere informazioni su Epicode utilizzando vari tool;

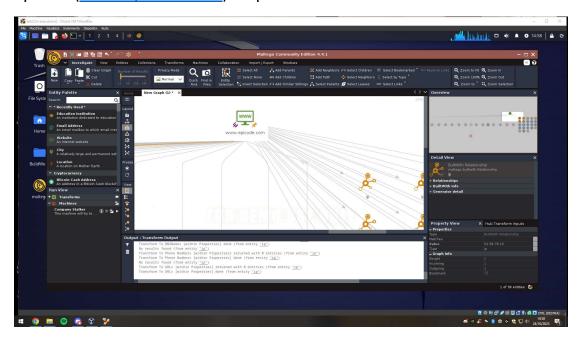
In un primo momento ho utilizzato Google cercando con la query Intitle:Epicode così da vedere tutte le pagine che hanno Epicode nel loro titolo. Con questa prima ricerca ho trovato queste informazioni.



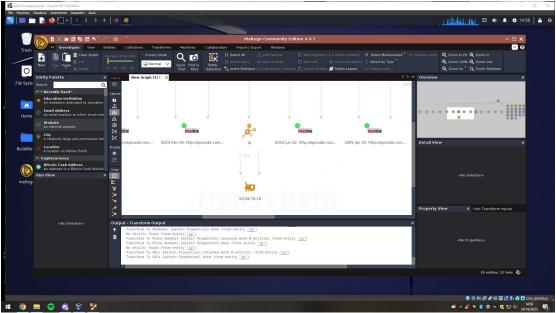
Sul fondo della home page ho trovato il codice fiscale dell'azienda che a sua volta ho utilizzato per cercare altre informazioni sempre su google. Infatti poi ho trovato sul sito dell'ufficio camerale tutte le specifiche dell'azienda Epicode come si può vedere dallo screen che segue.



Avendo queste informazioni più generali ma comunque utili, poi ho utilizzato Maltego per analizzare più a fondo il sito di Epicode(www.epicode.com). E questo è il risultato:



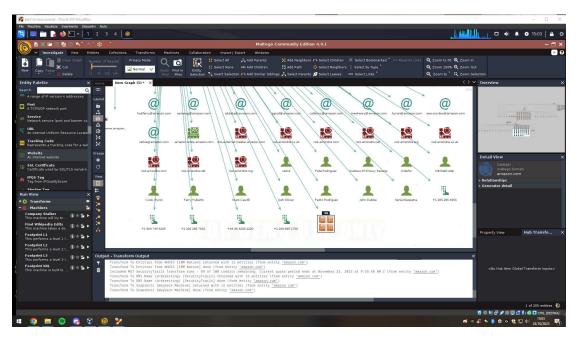






In questo ultimo screen possiamo vedere che epicode è collegato con la mail awsdns-hostmaster@amazon.com quindi possiamo supporre che Epicode utilizzi AWS di amazon come servizio cloud dei DNS che utilizza.

Andando più a fondo si vedono anche nomi e numeri di telefono, probabilmente, di persone che lavorano per questo servizio.



Nello screen successivo possiamo vedere come analizzando il DNS di www.epicode.info abbiamo estrapolato un indirizzo IP e un indirizzo MAC.



A sua volta interrogando l'indirizzo IP possiamo vedere che risulta arrivare dalla germania e ci mostra anche le porte che vengono utilizzate, questo vuol dire che probabilmente viene utilizzata una VPN o un proxy.

Nel prossimo screen, sul lato destro, possiamo vedere i dettagli dell'indirizzo IP in questione e possiamo vedere che Maltego sospetta che sia un indirizzo proxy.