O artigo *"How Unique is Your onion? An Analysis of the Fingerprintability of Tor Onion Services"* aborda a facilidade em identificar um utilizador que use *tor onion services*, que são serviços que permitem esconder a identidade online do utilizador, como por exemplo o WikiLeaks.

Este tipo de serviços permite que os utilizadores publiquem informações ou noticias que podem ser consideradas controversas na internet ou aceder a certos *websites* que tenham dados sensíveis sem que a sua identidade seja exposta. É explicado como pode ser feito o ataque na parte da rede que está mais vulnerável, que é um ataque que pode ser feito com poucos recursos e com alguma facilidade que tem bastante importância no contexto da rede e dos serviços em causa.

Em termos de aspeto negativos o artigo não aborta outros tipos de ataque, apenas o ataque que é possível realizar entre o utilizador e o primeiro *router* da rede *tor*, o que apesar de ser um ataque importante deixa muitos outros por elaborar. Os tais chamados ataques de ultima geração (state of the art attacks) são brevemente descritos, não explicando bem como são feitos. A rede *tor* permite que o atacante crie base de dados com informação sobre os acessos aos *website* ou *hidden services*.

Grupo TS12:

Francisco Caeiro, 47823

António Estriga, 47839