O artigo *"Who Left Open the Cookie Jar? A Comprehensive Evaluation of Third-Party Cookie Policies"* fala sobre um novo *framework* de avaliação de políticas de *third party cookies* e sobre os resultados obtidos com sua utilização em vários *browsers* e extensões. *Third Party Cookies* são *cookies* de um domínio que não é aquele que o utlizador está a visitar. O *Framework* funciona criando instâncias dos *browsers*, fazendo-os correr os casos anteriormente definidos e verificando os resultados.

Os resultados obtidos no caso dos *browsers* são bastante surpreendentes pois demonstram que o *browser* mais utlizado, o *Chrome*, não tem qualquer tipo de segurança contra a exploração destas vulnerabilidades exceto quando bloqueamos as *cookies* o pode tornar a navegação impossível. Também é surpreendente o facto da opção para bloquear *thrid party cookies* no *Edge* não tenha qualquer efeito prático. É também de elevada importância o facto de o *Safari* ser o único browser mainstream com boas resultados nas definições predefinidas. No caso das extensões os resultados ainda são piores pois não conseguem bloquear absolutamente nada devido as API utlizadas para comunicar com os *browsers*.

Os pontos negativos são a pouca informação sobre como foi feita a ferramenta e porquê, falta de informação sobre os sistemas operativos usados e a respetivas versões dos *browsers/release date* e falta de maneiras como evitar estes problemas devido a abordagem usada.

Em suma, este artigo mostra uma ferramenta que dia ser usada pelos *developers* destes *browsers* para verificar a segurança dos mesmos em relação a estas vulnerabilidades.

Grupo TS12:

Francisco Caeiro, 47823

António Estriga, 47839