

[Le FBI et Carnegie Mellon en cheville pour casser Tor](#)

En juillet 2014, une présentation sur les moyens de désanonymiser les utilisateurs de **Tor** sans se ruiner a été [annulée de la conférence Black Hat USA](#) qui se préparait. À l'époque, les avocats du **Software Engineering Institute** ou SEI de l'Université Carnegie Mellon (qui reçoit d'importants financements du Département de la défense américain) s'étaient opposés à la diffusion publique des travaux du chercheur Alexander Volynkin, qui devait intervenir avec l'analyste Michael McCord. Le doute quant au devenir et à l'utilisation effective de leur méthode pourrait être levé.

« Au moins 1 million de dollars »

Selon les animateurs du projet Tor, le **FBI** aurait grassement payé Carnegie Mellon pour obtenir la primeur des recherches et utiliser la technique lors d'une attaque constatée par le réseau d'anonymisation dès le premier semestre 2014. *« Apparemment, les chercheurs [de Carnegie Mellon] ont été payés par le FBI pour attaquer largement les utilisateurs de services cachés, puis passer au crible leurs données afin de trouver des personnes qui pourraient être accusées de crime »*, a indiqué dans un billet de blog du 11 novembre Roger Dingledine, co-développeur initial de Tor et directeur du projet. *« Nous avons appris que le paiement versé à l'Université Carnegie Mellon était d'au moins 1 million de dollars »*, de sources émanant de la communauté de sécurité, a-t-il précisé au magazine [Wired](#).

Une opération internationale

La technique des chercheurs de l'Université Carnegie Mellon (CMU) aurait appuyé l'[opération internationale de police Onymous](#) (Interpol, FBI...) menée contre plus de 400 services du darknet vendant des marchandises illégales, dont Silk Road 2. *« Les autorités en charge de l'application de la loi peuvent utiliser Tor pour mener leurs enquêtes de manière éthique – nous soutenons une telle utilisation de Tor –, mais une investigation ne saurait justifier l'invasion massive de la vie privée des gens, et certainement pas en se faisant passer pour une 'recherche légitime' »*, a insisté Dingledine. *« Quelle que soit la recherche universitaire de sécurité menée au 21ème siècle, a-t-il ajouté, elle ne doit pas inclure 'd'expériences' contre paiement qui mettent indistinctement en danger des individus sans leur consentement »*.

Lire aussi :

[Interpol s'entraîne à combattre le darknet](#)

[Tor à la recherche de financements moins gouvernementaux](#)

crédit photo © g0d4ather / Shutterstock.com