Le FBI a recruté chez Tor pour démasquer les utilisateurs

Tor trahi par un des siens. C'est très probable selon le Daily Dot et de nommer le traître qui a aidé le FBI à connaître l'identité des personnes naviguant sur le réseau anonyme Tor : Matthew Edman. Il a rejoint le projet comme développeur en 2008 alors qu'il était étudiant à l'Université Baylor. Il était en charge de travailler sur Vidalia, la création d'une interface graphique simple pour déployer et gérer les connexions Tor plus facilement. Ce projet a été abandonné en 2013

Matthew Edman, fort de son doctorat acquis en 2011, a alors commencé à travailler en 2012 pour Mitre Corporation en tant qu'ingénieur senior en cybersécurité. Cette structure est connue dans le monde de la sécurité informatique, car elle gère la base de données CVE (Common Vulnerabilities and Exposures) qui compile l'ensemble des vulnérabilités trouvées. Mais ce que l'on sait moins, c'est que Mitre Corporation travaille notamment pour la Défense américaine et d'autres agences pour en tirer un revenu annuel évalué à 1,5 milliard de dollars. Et selon le journal américain, le poste de Matthew Edman était de travailler avec le FBI pour trouver des moyens d'espionner de potentiels criminels. Dans ce cadre il a créé Torsploit (également connu comme le malware Cornhusker) en collaboration avec plusieurs agents du FBI.

Torsploit utilisé dans plusieurs opérations

L'agence fédérale s'est servie de ce malware pour l'opération Torpedo visant trois sites pédopornographiques sur le Darknet. Pour cela, elle avait encapsulé le logiciel de Matthew Edman dans un fichier Flash placé sur les sites en question. Le malware pouvait alors détecter les véritables adresses IP des visiteurs qui avaient activé Flash dans leur navigateur. Au final, 25 suspects et 19 personnes ont été condamnées. Depuis, le FBI s'est appuyé sur d'autres logiciels malveillants pour traquer les utilisateurs de Tor. Certains soupçonnent l'agence fédérale de détenir une faille dans le navigateur Tor lui-même, capable de fonctionner aussi sur Firefox. Pendant le procès sur l'affaire Torpedo, un des prévenus a demandé une expertise technique sur Torsploit. Le FBI a indiqué sans coup férir « avoir perdu le code source » du malware.

Matthew Edman a poursuivi sa collaboration avec le FBI en aidant au démantèlement de Silk Road. Après son aventure avec le FBI, il a rejoint Bloomberg, FTI Consulting et il est maintenant un des dirigeants de Berkeley Research Group en compagnie de 3 anciens agents du FBI et d'un procureur en charge de l'affaire Silk Road.

A lire aussi :

Pour CloudFlare, 94% du trafic du réseau Tor est malveillant

Le projet Tor renforce sa sécurité pour détecter les espions

Utilisateurs du navigateur Tor, méfiez-vous des souris !