GitHub nie tout piratage mais pas toute fuite de code source

GitHub doit-il revoir son système de signature des opérations de *commit* ? Son patron Nat Friedman vient en tout cas de prendre des engagements dans ce sens.

Il aura fallu un *bad buzz* pour en arriver là. En l'occurrence, la prétendue publication du code source de la plate-forme. À la baguette, un individu qui se dit « développeur TypeScript et défenseur de la vie privée ».

Dans un post intitulé « Qu'est-ce que Microsoft* pense vraiment de l'*open source* ? », il affirme avoir usurpé l'identité de Nat Friedman. Et publié le code source en question dans l'un des dépôts officiels de GitHub. Dépôt pas choisi par hasard, puisqu'il s'agit de celui où l'entreprise consigne les demandes de retrait de contenus qu'on lui fait au nom du DMCA. L'une d'entre elles, portant sur youtube-dl, a eu un fort retentissement ces derniers jours.

Le *leaker* autorevendiqué pointe, en guise de preuve de ses actions, vers une archive datée du 4 novembre. Ceux qui ont pu la consulter – elle n'est plus accessible – se seront demandé si le code exfiltré est à la fois celui de github.com et de GitHub Enterprise. Pour peu qu'il soit authentique, le *readme* pousse à répondre par l'affirmative.

GitHub le reconnaît, du code source a filtré

À la lumière des événements, Nat Friedman est intervenu sur le forum Hacker News. Son message : il n'y a pas eu de piratage. Ce qui ne signifie pas, admet le dirigeant, qu'il n'y a pas eu de fuite. « *Il y a quelques mois, nous avons accidentellement envoyé à certains de nos clients un tarball brouillé contenant le code source de GitHub Enterprise Server* », explique-t-il. Cette version *on-prem* de la plate-forme « a du code en commun avec github.com », ajoute-t-il sans préciser dans quelle mesure.

Et de recommander aux utilisateurs de systématiser la signature des opérations de *commit*. En l'état, Git, le logiciel de gestion de versions sur lequel repose GitHub, permet facilement de détourner celles qui ne le sont pas, explique Nat Friedman.
Dans le cas présent, une copie du dépôt DCMA a peut-être été mis en place. Avec l'idée d'exploiter deux propriétés de GitHub. D'une part, tous les *forks* reposent sur un même dépôt Git. De l'autre, les commits dans ces *forks* sont accessibles depuis ledit dépôt, à condition de connaître son hash.

** Microsoft est propriétaire de GitHub. Il en a fait l'acquisition en 2018 pour 7,5 milliards de dollars.*

Photo d'illustration © DASPRiD / CC BY 2.0