La Chine suspectée d'une violente attaque DDoS sur GitHub

GitHub, la plate-forme d'hébergement et partage de logiciels Open Source utilisée par 8 millions de personnes, subit une attaque massive depuis la fin de semaine dernière. La plus forte attaque DDoS de son histoire, indique l'entreprise américaine sur son blog. L'attaque a démarré le jeudi 26 mars pour s'intensifier les lendemain et surlendemain bloquant l'accès au service pour certains utilisateurs.

Une attaque qui évolue face aux contre-mesures

Une attaque visiblement bien maîtrisée puisqu'elle *« utilise une combinaison de vecteurs »*, indique la plate-forme. Des méthodes de distribution par dénis de service déjà éprouvées par le passé mais aussi *« de nouvelles techniques sophistiquées qui utilisent les navigateurs de gens non suspects et non impliqués pour inonder Github.com avec de fort niveau de trafic »*. De plus, la tactique des attaquants évoluait dans la journée en fonction des mesures prises pour atténuer l'afflux de requêtes malveillantes sur les serveurs web. Pendant tout le week-end, les équipes techniques de GitHub ont bataillé pour réduire, avec plus ou moins de succès, l'impact de la manœuvre. Laquelle n'avait toujours pas cessé ce lundi matin. *« L'attaque DDoS a évolué et nous travaillons à la limiter »*, indiquait la plate-forme de codage à 6h46 heure UTC (7h46 en France) sur sa page des statuts. Néanmoins, les applications serveurs étaient disponibles à plus de 99,9% ce lundi midi.

La manœuvre ne cherche apparemment pas à faire tomber la plate-forme Open Source mais viserait certains contenus. *« Nous pensons que l'intention derrière cette attaque est de nous convaincre de retirer un certain type de contenu »*, avance GitHub, sans préciser lequel. Selon les experts que le *Wall Street Journal* a interrogé, l'attaque proviendrait clairement de Chine. Et viserait à bloquer les outils de certains développeurs qui utilisent GitHub pour contourner la censure du pays.

La Chine pointée du doigt

C'est notamment le cas de GreatFire.org, une association de lutte contre la censure chinoise et dont les méthodes de *mirroring* des contenus ont inspiré la nouvelle campagne de RSF pour lutter contre la censure là-aussi. Les experts en sécurité ont en effet constaté qu'un énorme volume de requêtes passaient par le moteur de recherche chinois Baidu. Une information que GitHub n'a pas confirmée ni précisé si GreatFire.org était effectivement la cible de l'assaut. Toujours selon le quotidien américain, Baidu déclare ne pas être impliqué dans l'attaque ni que ses serveurs ont été détournés.

Mais pour Mikko Hyponen, responsable en chef technique de F-Secure, l'attaque est probablement orchestrée par les autorités chinoises qui disposent de la capacité à manipuler le trafic web à un haut niveau de par la structure même du réseau Internet de la région. *« C'est quelqu'un qui a la capacité de toucher à tout le trafic Internet en Chine »*, déclare-t-il. Une nouvelle méthode où les forces vives numériques du pays servent une même cause en quelque sorte…

Lire également

Le gouvernement allemand ciblé par des attaques DDoS

iCloud victime d'une attaque de l'homme du milieu en Chine ?

Sécurité : portrait-robot des attaques DDoS (infographie)

crédit photo © Duc Dao – shutterstock