

# [Git.psi.i2p : un GitHub à la sauce Dark Web](#)

Nos confrères de *Softpedia* ont déniché sur le Dark Web un service d'hébergement et de gestion de développement de logiciels, nommé git.psi.i2p. Ce dernier s'apparente à GitHub, plateforme connue dans le web visible. Ce clone repose sur Gogs, un système codé en Go pour crée des repository en ligne.

Git.psi.i2p a une petite particularité par rapport à GitHub, il ne fonctionne qu'avec le réseau Tor ou plus récemment I2P, pour garantir une anonymisation complète. Jeff Becker, à l'origine de cette solution a expliqué à nos confrères journalistes ses motivations : *« J'ai élaboré ce service pour voir si le logiciel que j'avais créé fonctionnait et, depuis, je l'ai mis à disposition de ceux qui souhaitent l'utiliser. »*

Ce service a été lancé il y a deux semaines et ne fédère aujourd'hui que 30 à 40 utilisateurs. Il n'héberge que 43 applications dont 14 proviennent de Jeff Becker lui-même. Un score modeste, mais encourageant pour un système caché dans les ténèbres du web.

## Des risques de dérapages assumés

Bien évidemment avec ce type de plateforme, la question du type d'applications hébergées se pose. Elle pourrait attirer des développeurs qui ont déjà eu des problèmes pour stocker leurs codes sur GitHub. En mars dernier, ce dernier a été victime [d'une attaque par déni de service relativement violente](#). Elle a été orchestrée par la Chine et visait à bloquer les outils de certains développeurs qui utilisent GitHub pour contourner la censure du pays, le Grand Firewall.

Jeff Becker est conscient de ce problème. *« J'ai pris des règles pour ne pas avoir du « porn d'aucune sorte » pour garder ce lieu le plus professionnel. »* Et d'ajouter *« qu'il est interdit d'utiliser le Git pour les Commandes et Contrôle des botnets »*. Il ne voit par contre *« pas de problème avec le code source de malware, mais uniquement dans un cadre de proof of concept, à des fins de recherches ou d'apprentissage »*. Il relativise aussi le danger. *« Certains développeurs de malware ne réalisent pas et ne soucient pas que les gouvernements peuvent aussi utiliser leur malware. »* Il reste pragmatique en assurant qu'il ne faut pas stigmatiser les services utilisant les réseaux d'anonymisation. *« Contrairement à la croyance populaire, ces réseaux apportent plus de sécurité pour les utilisateurs réguliers que de faciliter la vie des « mauvais » utilisateurs. »*

### A lire aussi :

[Dark Web : les données volées bénéficient d'une diffusion accélérée](#)  
[Avec Memex, la Darpa scrute les tréfonds de l'Internet](#)

**Crédit Photo : Olly-Shutterstock**