Une marketplace du Dark Web lance un bug bounty

Faut-il y voir une concordance des temps ? Hier, nous nous faisions l'écho des Anonymous débranchant 20% du Dark Web en s'attaquant à l'hébergeur Free Hosting II. Le collectif de pirates a réussi à bloquer plus de 10 000 sites en .onion, les défacer et voler la base de données. Un exploit qui a donné matière à réflexion à plusieurs autres places de marché de la face cachée du Web.

Parmi elles, on retrouve Hansa, un portail où les utilisateurs peuvent acheter et vendre des produits illégaux comme des malwares, des données volées, des armes à feu, des drogues, etc. Or, cette marketplace vient de lancer un programme de recherche de bugs pour contrer les pirates, mais aussi les investigations des autorités judiciaires pour identifier et désanonymiser les propriétaires et les utilisateurs du site.

Un bug bounty pour mieux se protéger

Ce bug bounty a été lancé la semaine dernière, mais Hansa en a fait la promotion depuis hier sur son site et via un post publié sur Reddit. Selon le message, les administrateurs de Hansa sont disposés à payer jusqu'à 10 bitcoin (soit environ 10 200 dollars). Les autres rétributions sont de 1 bitcoin (environ 1000 dollars) pour un exploit non critique ou des failles pouvant rendre le service hors ligne, ainsi que 0,05 bitcoin (50 dollars) pour de simples bugs d'affichage. Un niveau de récompense similaire à ceux proposés par les acteurs de la Silicon Valley via leur programme officiel de recherche de bugs.

La place de marché fixe comme ses homologues du Web des conditions pour être éligible à une récompense. Les attaquants ne doivent pas provoquer d'interruption de service du site principal. Ils ne doivent pas non plus accéder aux comptes des utilisateurs. La démonstration de bugs n'est valable que sur des comptes tests.

Cette initiative intervient au moment où un magasin du Dark Web, AlphaBay, a payé une rançon à un pirate qui a trouvé une faille, lui permettant de lire plus de 218 000 messages privés contenant des informations sensibles comme les adresses de livraison, des identifiants de portefeuilles de bitcoin et des numéros de suivi de colis.

A lire aussi :

Le Bug Bounty de l'US Army trouve une faiblesse du réseau interne

Sécurité : l'Europe inclut un bug bounty à son audit logiciel

Crédit Photo : Releon8211-Shutterstock