Snowpack rend invisible l'échange des données sur l'internet

Description

Snowpack, une start-up située à Paris et à Vienne, opère un réseau informatique appelé Snowpack Network Overlay, un « réseau d'invisibilité permettant de garantir l'anonymisation et la sécurisation des données », même avec l'arrivée des ordinateurs quantiques. Le projet, lancé en 2016, d'abord en incubation au Commissariat à l'énergie atomique (CEA), est devenu une entreprise en mai 2021, avant de lever 2 millions d'euros en novembre 2022.

Aujourd'hui, lorsque deux personnes communiquent *via* le réseau internet, le contenu de leur échange circule sous la forme de paquets de données acheminés par les protocoles IP (Internet Protocol) qui fournissent une méthode pour les mener à destination. Si le contenu d'un échange peut être crypté, les métadonnées conduisant son acheminement restent visibles, notamment l'adresse IP de l'expéditeur et celle du destinataire. Pour sécuriser une communication sur les réseaux, des techniques de cryptage du contenu sont le plus souvent utilisées entre l'expéditeur et le destinataire, mais les métadonnées restent un point de vulnérabilité majeur, exploité par ceux qui « écoutent » le réseau, notamment ceux des États qui en ont les moyens.

Une approche alternative, explorée depuis le début des années 2000, fait l'objet d'un grand nombre de publications et de dépôts de brevets. Cette méthode « *consiste à faire circuler des informations complémentaires sur des voies distinctes* », explique le CEA. Pour Frédéric Laurent, cofondateur et président de Snowpack, « *pour attaquer un contenu, il faut d'abord pouvoir l'identifier* ». Partant de ce principe, la technologie développée par Snowpack consiste à envoyer le contenu d'une communication en « fragments complémentaires », appelés « flocons », qui sont anonymisés et qui empruntent, sur le réseau, des chemins séparés, également créés de manière anonyme. Ce réseau est composé de nœuds exploités par Snowpack, par ses clients exigeant le plus haut niveau de sécurité et également par des opérateurs indépendants. « *Sur ces chemins, nous ne faisons pas transiter de paquets IP, mais ce qu'on appelle des flocons, c'est-à-dire du bruit qui a une taille standardisée. Si une personne malveillante prend la main sur l'un des flocons, elle doit retrouver parmi l'ensemble des autres celui qui est son « complément » pour pouvoir accéder à la donnée. En pratique, pour recomposer une milliseconde de flux, même sans qu'aucun de ces flux ne soit chiffré, il faudrait plusieurs années* », explique Baptiste Polvé, cofondateur et directeur technique de Snowpack.

Cette solution inédite permet de rendre invisible tout à la fois les appareils utilisés pour communiquer, le contenu de la communication et les métadonnées nécessaires à leur acheminement. La technologie a nécessité cinq ans de recherche et de développement au sein du CEA-List et bénéficie de trois brevets exclusifs déposés dans le domaine de la cybersécurité. L'un des avantages du réseau Snowpack est de ne pas

dépendre d'un tiers de confiance pour établir les communications. La solution se présente comme étant résistante aux outils de surveillance de masse des réseaux, déployés par les États. « *Un attaquant utilisant des sondes « industrielles » classiques sur le réseau dorsal aura certainement une forte probabilité de « voir » les fragments complémentaires, mais comme ils sont anonymes et similaires (même taille, pas de contenu intelligible), il devra les recombinaison avec tous les autres pour identifier les complémentarités. Comme la factorielle du trafic croît beaucoup plus fortement que la capacité de calcul, une attaque par force brute devient irréaliste* » explique Frédéric Laurent. De plus, les communications devenant « invisibles » sur le réseau, le réseau Snowpack anticipe l'arrivée prochaine des ordinateurs quantiques capables de casser les algorithmes de chiffrement actuels. Snowpack serait alors une solution « post-quantique » originale ([voir La rem n°63, p.38](#)).

En outre, Snowpack figure parmi les onze acteurs français spécialistes en cybersécurité du projet collaboratif SCRED (Socle commun du renseignement cyber et de détection), piloté par Thales depuis avril 2023, et financé par l'État dans le cadre de France 2030. L'objectif de SCRED est de créer, d'ici trois ans, une plateforme unique pour les entreprises et les administrations publiques afin de leur proposer « *des technologies innovantes, essentielles à la garantie de la souveraineté de la France* » explique Thales. En novembre 2022, l'entreprise d'une dizaine de personnes a levé 2 millions d'euros, notamment auprès de Bpifrance, Arion.vc, Itera Invest et EIT Digital (cofinancé par l'Union européenne).

Ce réseau qui rend invisible l'échange des données sur internet s'adresse tout particulièrement aux entreprises de défense, de cybersécurité et d'investigation numérique, qui doivent au demeurant montrer patte blanche avant de devenir client, puisque personne ne sera en mesure d'intercepter ou d'écouter les données, pas même Snowpack.

Sources :

- Snowpack, snowpack.eu
- Philippe Richard, « Pour contrer le cyberespionnage, la start-up Snowpack propose de cacher les informations dans des « flocons » », techniques-ingenieur.fr, 7 janvier 2022.
- Paul Loubière, « Le CEA veut son ordinateur quantique dans deux ans et investit des millions pour cela », challenges.fr, 12 décembre 2022.
- « Snowpack, solution inédite d'anonymisation et de sécurisation des données », Commissariat à l'énergie atomique, cea.fr, 25 janvier 2023.
- « Thales lance la plateforme française de renseignements sur la menace cyber pour une plus grande autonomie et une résilience renforcée avec 10 autres acteurs français », Thales, thalesgroup.com, 5 avril 2023.

Categorie

1. Techniques

date créée

19 septembre 2023

Auteur

jacquesandrefines