3 QUESTIONS À...
MARS 2024

Olivier Morel, directeur général adjoint de Snowpack

DEVENIR INVISIBLE POUR CONJURER LES ATTAQUES CYBER

Une cape d'invisibilité pour contrer les sortilèges de la cybercriminalité et diminuer la surface d'attaque des systèmes d'information afin de la cacher aux pirates informatiques, c'est la technologie de rupture imaginée, brevetée et développée par Snowpack. En moins de trois ans d'existence, cette Start-up issue du CEA a déjà reçu plusieurs récompenses. Lauréate I-lab 2022, soutenue par la Stratégie d'accélération cyber et DeepNum20, elle vient également de remporter le grand prix de la Start-up au Forum in Cyber 2024. Si sa notoriété est basée ur l'anonymisation et l'invisibilité sur Internet, cette société présentée par son directeur général adjoint, Olivier Morel, compte bien se faire un nom dans le milieu de la cybersécurité !

Pouvez-vous nous présenter Snowpack, dont l'appellation révèle en partie l'originalité de la technologie déployée ?

« *Spin off issue* du Commissariat à l'énergie atomique et aux énergies Alternatives (CEA), Snowpack a développé une solution inédite d'anonymisation et d'invisibilité sur internet. Son concept de base, protégé par 4 brevets internationaux exclusifs déposés dans le domaine de la cybersécurité, est de dire que si les attaquants ne vous voient pas, ils passeront leur chemin. Cette promesse de devenir indétectable est basée sur deux postulats : « pour vivre heureux, vivons cachés », morale d'une fable de Florian intitulée *Le Grillon,* et il est impossible de faire confiance à qui que ce soit, même pas à Snowpack (*rires*). N'étant pas tiers de confiance, notre technologie vous garantit que personne n'accédera à vos données, et même pas Snowpack ! Elle évite ainsi toute dépendance à des technologies qui ne sont jamais totalement invulnérables et qui peuvent être compromises à tout moment par des personnes malveillantes. Portés par ce principe, les fondateurs, des anciens salariés du CEA, ont mis au point un procédé très différent des mécanismes de chiffrement utilisés par les VPN par exemple. Cette innovation de rupture s'appuie sur un réseau invisible - une surcouche réseau ou « Network Overlay » - dans lequel les données sont fragmentées en petits paquets et envoyées sur différentes routes à travers ce réseau. Appelés flocons, ils sont comparables à des bruits aléatoires, qui, en cas d'interception, sont totalement inexploitables. Elles sont ensuite reconstituées pour arriver à leur destination finale. »

À qui s'adresse cette cape d'invisibilité aux pouvoirs presque magiques ?

« La technologie de rupture Snowpack, appelée « VIPN » (Virtual Invisible Private Network), se décline en trois offres logicielles : **Invisible access** protège l'activité des utilisateurs ayant - par exemple - recours à internet dans des zones géographiques à risque ou ayant un besoin très élevé d'anonymat. Elle leur donne la possibilité de naviguer sans laisser de traces. **Invisible Services** permet de cacher l'accès aux services web les plus sensibles, afin de ne les rendre accessibles qu'aux seuls utilisateurs ayant le droit d'y accéder. Enfin, **Invisible Infra** masque les composants d'infrastructure du système d'information exposés sur Internet afin de les protéger. Pour clarifier, on peut comparer le système

d'information à un château fort doté de plusieurs portes. Même si elles sont très bien sécurisées, l'attaquant peut quand même les identifier et se procurer les moyens de forcer les serrures pour parvenir à entrer. Avec Snowpack, il est impossible de voir ces portes. Tout danger d'intrusion est donc éliminé.

Facile à installer et à déployer, la solution dispose d'atouts majeurs. Elle est très peu intrusive et adaptée à tout type d'organisation. Bénéficiant de mises à jour et d'évolutions, elle demande très peu d'exploitation ou de supervision, et pour l'intégrer inutile de changer tout son SI ! »

> **La technologie Snowpack apporte aux établissements de santé l'opportunité de rendre invisible leur surface d'attaque externe des pirates informatiques.**

En quoi cette solution est-elle adaptée aux établissements de santé ?

« Pour le secteur de la santé en particulier, nos offres Invisible Services et Invisible Infra permettent de réduire considérablement la surface d'attaque externe des systèmes d'information hospitalier, de plus en plus étendues, ouvertes, et donc vulnérables. Considérant la situation des établissements hospitaliers en termes de cybersécurité, nous pouvons leur faire gagner un confort et un temps considérables. D'autant plus que les attaques ne viennent pas que de l'extérieur. Cliniques et hôpitaux sont à la merci d'intrusions internes, de compromissions de collaborateurs, d'erreurs humaines, de tentatives de phishing et de rançongiciels qui sont déjà nombreuses. En revanche, cachés du monde extérieur par la bulle d'invisibilité conçue par Snowpack, ils pourront continuer de mener leur travail de sensibilisation et de renforcement de leur niveau de sécurité informatique interne. Nous amenons donc au secteur de la santé un nouveau paradigme, qui va sûrement donner de l'air et de l'espoir à un écosystème très attaqué et confronté à des chantiers assez insurmontables en matière de cybersécurité ! »

3 QUESTIONS À...

BIO EXPRESS

Directeur général adjoint de Snowpack depuis septembre 2023, Olivier Morel a travaillé 18 ans chez un éditeur de logiciel spécialisé dans des solutions de cybersécurité.
Membre du conseil d'administration et trésorier d'Hexatrust, il est très investi dans cette association qui fédère aujourd'hui 130 PME, ETI et start up de la cyber et du cloud de confiance.

Doshas Consulting
128 rue La Boétie 75008 Paris
+33 (0)1 84 20 27 83
contact@doshas-consulting.com
www.doshas-consulting.com

Conception : Doshas Consulting
Responsable de la publication : Didier Ambroise
Rédaction : Cécile Jouanel
Conception, réalisation : Studio Bleu Canari