34 EDITION QUOTIDIENNE DU 18 NOVEMBRE 2020 NUMERIQUE

CYBERSECURITE : COMMENT LA STARTUP CROWDSEC CREE LE "SYSTEME IMMUNITAIRE" DU WEB

SYLVAIN ROLLAND

La startup nantaise a développé une technologie unique sur le marché capable de repérer de bloquer les adresses IP malveillantes qui visitent les sites et applications de ses utilisateurs. Elles sont ensuite partagées en open source et bloquées par tout le réseau, créant une "immunité collective". L'outil, gratuit pour l'instant, est déjà utilisé dans une vingtaine de pays. Une version payante pour les entreprises sera lancée début 2021.

Contrairement au Covid-19, il ne pourra jamais exister de vaccin pour protéger les machines, les sites, les applications et les objets connectés à Internet, des attaques des pirates informatiques. Alors, la startup nantaise CrowdSec travaille sur l'immunité collective. Son crédo : traquer les adresses IP malveillantes qui tentent d'infecter les sites ou applications de ses utilisateurs. Sa méthode : analyser les "*logs*", ces journaux d'activités remplis de données précieuses sur le comportement des internautes.

> *"Chaque comportement laisse des traces et c'est de l'or pour nous, explique Philippe Humeau, le cofondateur de la startup. Par exemple, un pirate qui tente de détecter votre mot de passe va devoir faire plein d'essais. Mais comme notre logiciel est capable de détecter les comportements suspects, il s'en aperçoit très vite et le bloque avant qu'il réussisse", détaille l'ancien hacker "blanc", c'est-à-dire qu'il mettait ses compétences au service des entreprises plutôt que contre elles.*

Et pour créer cette immunité collective, CrowdSec utilise le pouvoir de la multitude. Chaque adresse IP est immédiatement partagée à tout le réseau d'utilisateurs de la solution, assortie d'un score de réputation. Celles qui sont malveillantes sont immédiatement bloquées.

Le concept a convaincu le fonds Reflexion Capital, qui a mené cette année une levée de fonds de 700.000 euros en embarquant des investisseurs prestigieux comme Thierry Rouquet, fondateur des startups en cybersécurité Sentryo et Arkoon. A cet argent s'ajoutent 600.000 euros de prêts bancaires et 200.000 euros de la part de business angels, soit au total 1,5 million d'euros pour "développer le produit et la communauté" dans l'année à venir.

Lire aussi : "Cultiver" plutôt que "acheter" pour faire face à la pénurie d'experts en cybersécurité

LE "WAZE" DE LA CYBERSÉCURITÉ

Fondée en janvier 2020 par les entrepreneurs Philippe Humeau, Thibault Koechlin et Laurent Soubrevilla, tous trois issus de grandes écoles d'ingénieur, CrowdSec est donc une plateforme d'automatisation de la cybersécurité qui repose sur deux piliers : l'analyse comportementale et la réputation des adresses IP. Son objectif est de créer la **première solution collaborative pour sécuriser en temps réel et de manière préventive tout ce qui peut se connecter à Internet**, et donc être la cible d'attaques informatiques.

> *"Nous voulons rendre la cybersécurité accessible au plus grand nombre et à moindre coût, et créer la plus grande base de données réputationnelle au monde", déclare Philippe Humea*

Pour cela, pas de secret : la startup doit faire grossir sa communauté, et vite, car plus l'outil conna d'adresses IP, plus il est efficace. "*Notre force, c'est la multitude : c'est de pouvoir dire à nos futur clients qu'on sait repérer tous les comportements suspects auxquels ils peuvent être confrontés, e empêcher ces attaques*", poursuit l'entrepreneur.

Aujourd'hui, CrowdSec (littéralement *crowd security* ou la sécurité par le nombre) revendique plus de 1.000 d'utilisateurs sur GitHub -la principale plateforme des développeurs-, particuliers ou entreprises, répartis dans une vingtaine de pays. Ceux-ci installent la solution et laissent le logiciel scanner tout ce qu'il se passe autour de lui et proposer un certain nombre de scénarios probables d'attaque. Dès que l'outil repère une adresse IP suspecte, celle-ci est remontée dans la base de données centrale de CrowdSec, et partagée avec les autres utilisateurs.

Pour l'heure, la solution est gratuite. "*A partir de 10.000 utilisateurs sur GitHub, on ne sera plus rattrapables car notre base de données sera trop énorme, c'est le seuil qui déclenche l'effet boule de neige*", affirme avec confiance Philippe Humeau, qui revendique une croissance organique forte.

Les développeurs qui contribuent à enrichir la base de données peuvent profiter gratuitement de la plateforme, mais la startup prépare une version professionnelle payante, qui sera disponible début 2021, pour les entreprises qui souhaitent simplement utiliser CrowdSec pour se protéger des attaques. La startup se revendique conforme au RGPD, le règlement européen sur la protection des données.

Lire aussi : Fuites de données : CybelAngel lève 34 millions d'euros pour protéger les grands groupes

"CROWDSEC, C'EST MON DERNIER CASSE"

A 45 ans, Philippe Humeau affiche la confiance de l'entrepreneur multirécidiviste sûr de son coup. Après son diplôme de la prestigieuse Epita -tout comme son compère Laurent Soubrevilla-, l'ancien hacker a fondé en 1999, dès sa sortie d'école, l'entreprise de cybersécurité NBS System, revendue en 2017 au groupe français Oceanet Technology. Il a aussi investi dans d'autres pépites comme Akeneo et réalisé des missions de conseil en cybersécurité. Fort de ces expériences, le quadra vit sa nouvelle aventure entrepreneuriale comme "*un coup de force avec des amis*", tout aussi chevronnés que lui.

> *"CrowdSec c'est mon dernier casse, lâche-il dans un sourire. Tout ce que j'ai fait jusqu'ici m'a mené à ce projet. Ce n'est pas une future licorne, même si ça ne plaira pas à Cédric O. C'est une B to sale [une entreprise créée pour être rapidement revendue, ndlr]. On a une technologie unique au monde, qui répond à un vrai besoin. Quand notre radar à hackers en temps réel sera suffisamment précis, tout le monde va se l'arracher et on vendra l'entreprise à un géant", affirme-t-il en se fixant un horizon à cinq ans.*

Et ensuite ? L'entrepreneur se reconvertira dans "l*e journalisme ou l'enseignement*". En attendant, il travaille d'arrache-pied et s'entoure d'une "*équipe d'experts de top niveau*". Laurent Soubrevilla, cofondateur et directeur des opérations, a déjà monté trois entreprises (intelligence artificielle, marchés financiers, salons virtuels) et s'occupe à la fois de la gestion financière et du développement de la partie "automatisation" de la plateforme. Le troisième cofondateur, Thibault Koechlin, le directeur technique diplômé de l'Epita, a fait partie de l'aventure NBS System. "*C'est un petit génie du logiciel avec une grande préoccupation éthique et un sens aiguisé du business*", décrit Philippe Humeau. Les six autres employés de la structure sont tous des experts tech.

La feuille de route est claire : investir pour améliorer le produit (détection anticipée des menaces, prévision de comportements...) et la gestion par la data de l'immense base de données. En 2022, CrowdSec prévoit d'intégrer l'intelligence artificielle à son logiciel.

> *"Ce qui nous distingue d'un antivirus ou d'un pare-feu classique, c'est que nous détectons des comportements. L'étape d'après sera de les anticiper avec l'IA grâce aux signaux faibles que nous décelons dans notre analyse des logs. Par exemple, si une IP A, une IP B et une IP C passent à quinze minutes d'écart pour tenter de casser une sécurité, lorsque A repasse, l'IA va bloquer proactivement l'IP B et l'IP C", détaille l'entrepreneur.*

Un exemple parmi d'autres des multiples scénarii d'attaques que saura anticiper le logiciel.

Lire aussi : Quand les "hackers éthiques" de YesWeHack profitent du regain du télétravail