Covid-19 : Comment CybelAngel a neutralisé une escroquerie visant un fabricant de vaccins

L’expert français de la cybersécurité CybelAngel, qui vient d'intégrer l’indice Next40, collabore avec un groupe pharmaceutique à l’origine d’un vaccin contre le Covid-19. En mars 2020, la startup a signalé au FBI une fraude orchestrée par un groupe de hackers qui extorquait argent et données personnelles aux citoyens américains en imitant le site du laboratoire.

Temps de lecture : minute

---

8 avril 2021

Republication du 9 février 2021

Mars 2020. La pandémie de Covid-19 arrivait tout juste en Europe, après avoir émergé en Chine quelques mois plus tôt. En coulisses, les groupes pharmaceutiques s’activaient déjà dans l’espoir de trouver un vaccin. Profitant de l’anxiété des populations touchées par des mesures visant à limiter la propagation de ce nouveau coronavirus, les hackers ont tout de suite compris que la crise qui se dessinait pouvait devenir très rentable pour leurs affaires. La startup française CybelAngel, qui vient de faire son entrée dans l’indice Next40 ce lundi 8 février 2021, a détecté une tentative de fraude liée à la marque d’un des laboratoires les plus en avance dans la course au vaccin. Pour *Maddyness*, elle revient sur cette expérience sans pouvoir divulguer le nom pour des raisons de confidentialité.

Un principe actif à protéger

Fondée à Paris en 2013, CybelAngel dispose de bureaux aux États-Unis depuis deux ans. "*Je pensais que nous aurions à faire face à un délit de sale gueule, dans le sens où les Français sont connus pour les produits de luxe et moins pour des services informatiques*, raconte Erwan Keraudy, président-directeur général et co-fondateur de la startup, qui précise travailler pour des groupes de plus de 1 000 salarié·e·s. *Mais il n'en est rien : tout est allé très vite avec les secteurs de la banque, des télécoms et donc des pharmaceutiques* " . La jeune pousse tricolore sait aiguiser l'intérêt de ses prospects : elle les approche en proposant de scanner gratuitement le Web en quête d'informations à leur sujet. "*Il n'y a pas d'installation à réaliser, le nom de la marque suffit*" , indique le dirigeant.

C'est de cette façon qu'a procédé CybelAngel avec l'un des laboratoires pharmaceutiques qui occupe le devant de la scène ces derniers mois. "*À la mi-mars 2020, ce dernier nous a indiqué disposer d'un principe actif amené à devenir l'un des plus recherchés au monde*" , expose ainsi Erwan Keraudy, à qui l'on a demandé de s'assurer que ce dernier soit correctement protégé. La jeune pousse parisienne est en mesure d'ingérer "*des milliards*" de données DNS (Domain Name System). Ce qui permet d'identifier toutes les requêtes dont l'intitulé est similaire au nom d'un client, puisqu'une IA calcule par exemple la probabilité que des lettres composant le nom d'une marque soient inversées dans un nom de domaine – c'est ce qu'on appelle des "twists" dans le domaine.

À lire aussi
Les attaques informatiques criminelles ont explosé en 2020

Au moins 100 millions de dollars extorqués

CybelAngel a ainsi relevé qu'un serveur était en cours de mise en place par un groupe de hackers bien informés. Avec une technique de copycat : "*Le site qu'ils ont bâti ressemblait en tout point à celui du client, à une page près*". Ce dernier a été en ligne pendant 24 heures, laps de temps durant lequel les criminels ont extorqué des particuliers américains. "*On leur promettait d'être prioritaire pour la vaccination. Ils n'avaient qu'à compléter une fiche de renseignement à leur sujet, comportant des informations personnelles comme leur lieu de résidence, ainsi qu'à verser une certaine somme afin de réserver leur place*" , note Erwan Keraudy. Une campagne d'e-mailing a été mise sur pied pour appâter la population américaine.

Contactée par CybelAngel, l'entreprise qui hébergeait le site incriminé n'était "*pas réactive*". La startup tricolore a donc pris les devants et directement contacté le FBI (Federal Bureau of Investigation). "*Nous les avons alertés un vendredi soir. Une opération a été menée le week-end*

suivant, débouchant sur la saisie du serveur concerné" , affirme Erwan Keraudy, qui précise que le groupe de hackers avait déjà réussi à collecter "*100 millions de dollars au moins*" auprès de particuliers. Désormais, la page web qui permettait aux criminels de commettre leurs exactions arbore le sceau de l'agence américaine. "*C'est dans ces cas de figure que je me réjouis d'être dans la cybersécurité. Nous sommes une entreprise, certes. Mais nous œuvrons pour le bien de l'humanité en protégeant la propriété intellectuelle de nos clients* [les vaccins anti-Covid étant un bien précieux sur le plan sanitaire, N.D.L.R.]" , juge le dirigeant, selon qui l'attaque contrecarrée "*aurait été orchestrée par un État tiers*". Plusieurs institutions soupçonnent la Russie et la Chine d'être derrière ce type de cyberattaques ciblées.

À lire aussi
Bercy vous permet de tester en ligne votre cybersécurité

Se développer aux États-Unis, une priorité

CybelAngel, qui dispose de 120 salarié·e·s, ambitionne de "*tripler*" ce

chiffre d’ici à 2023. La jeune pousse a fait du marché américain, "*12 fois plus gros que la France*" , sa priorité. Son dirigeant, qui habite à New York depuis 2 ans, estime que l’entrée dans l’indice Next40, porté par le gouvernement, confère une "*force de frappe à l’étranger en s’appuyant sur la marque France*". "*C’est aussi un bon moyen d’institutionnaliser notre activité. Notre compétence est connue, car nos prospects contactent nos clients pour évoquer les résultats. Mais, dans l’imaginaire collectif, on reste des gens en sweat à capuche dans un garage*" , plaisante Erwan Keraudy, forçant le trait.

Au-delà de sa solution permettant de scanner 5 différents paramètres (noms de domaine, cloud, objets connectés, identifiants et dark web), CybelAngel proposera une offre visant à "*déterminer le périmètre à protéger*" chez ses clients. "*On se rend compte que les grands groupes, tentaculaires, ne savent pas précisément ce qui est couvert et nous faisons donc l’état des lieux*" , indique le chef d’entreprise. Et la startup ne devrait pas manquer de chantiers : alors que le télétravail s’est généralisé afin d’éviter la propagation du Covid-19, cette pratique constitue l’un des points de friction majeurs en matière de fuites de données – tout comme le nombre de collaborateur·rice·s et l’avancée de la migration vers le cloud.

Article écrit par Arthur Le Denn