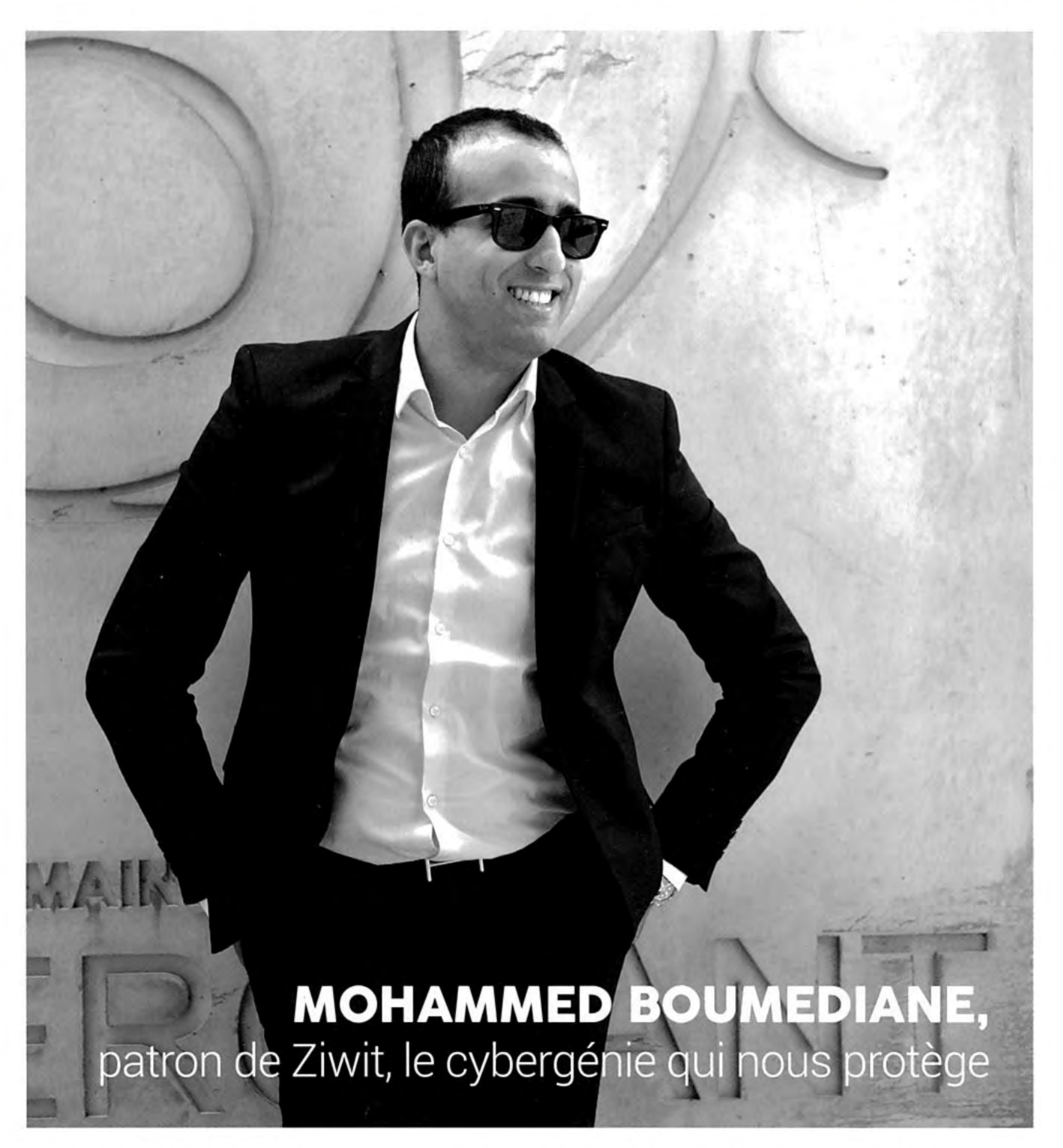
7 OFFICIEL METROPOLITAIN

INTERVIEW I ECONOMIE I POLITIQUE I CULTURE I ANNONCES LÉGALES

#1869 - 3 OCTOBRE 2017 - 1,50 €



MOHAMMED BOUMEDIANE,
patron de Ziwit, le cybergénie qui nous protège

FRENCH TECH
#Techthefutur accélère les projets

LOI DE FINANCES 2018
Qu'est-ce qui change ?

FESTIVAL
IG 2017

Texte : @GilMartin Photos : @Mario Sinistaj

Mohammed Boumediane

Le cyber génie

En 2011, à Montpellier, un jeune ingénieur marocain expert en cryptologie crée sa start-up, Ziwit, devenue en 2017 le leader européen de la cyber-sécurité. Mohammed Boumediane, son fondateur, est un génie et le cauchemar des hackers du monde entier. Avec les solutions HTTPCS développées discrètement à Montpellier, il a créé un bouclier qui protège serveurs et PC des attaques les plus sophistiquées. Ziwit protège déjà les ¾ des entreprises du CAC 40 et des Etats, dont la France et les Etats-Unis. Avec six filiales et 10 000 clients, Ziwit a un bel avenir : en matière de cybercriminalité, en effet, le pire est encore à venir... "Mais la lutte contre la cybercriminalité peut aussi devenir un formidable levier pour Montpellier", prévient Mohammed Boumediane en lançant Stratinvest, un fonds d'investissement de 6 M€ pour accompagner des projets en lien avec la défense et la cyber-défense. Rencontre avec un cyber-génie dont l'intelligence n'a rien d'artificiel.

DOMAINE
ERC
ANT
EL & SPA
DOMAINE DE
VERCHANT
★★★★ HOTEL & SPA

Comment Ziwit est-elle devenue un acteur mondial reconnu de la lutte contre la cybercriminalité ?

Je ne veux pas être trop technique et je ne peux pas non plus, pour des raisons évidentes, donner trop de détails (rires) : mais je peux dire que Ziwit a été la première start-up à développer des technologies offensives. Nos solutions en mode SAAS, commercialisées sous la marque HTTPCS, testent tous les jours, quasiment en permanence, les systèmes d'information et de protection de nos clients pour détecter les failles de sécurité de leurs sites web et de leurs applications. En fait, pour faire simple, nos programmes tentent de s'introduire dans leurs systèmes comme s'ils avaient l'intention de les pirater.

En fait, vos systèmes tentent de craquer les ordinateurs de vos clients ?

C'est un peu le principe, sauf que dans l'histoire, nous sommes les gentils ! Cette technologie, qui nous a pris deux ans de R&D, permet non seulement de repérer les failles mais aussi de les boucher. Le client est bien sûr informé en temps réel de l'intervention. Le recours aux techniques offensives est devenu incontournable car les virus sont de plus en plus intelligents. On l'a vu avec l'attaque sur Yahoo ! qui s'est fait voler des milliards de mails, ou, pendant les élections présidentielles, le piratage d'En Marche. Le phénomène s'intensifie.

Qui sont vos clients ?

Je peux citer Adobe, Oracle, Sales Force, TripAdvisor, LinkedIn ou Google. Mais nous avons aussi des pays de l'Otan, et d'autres états encore. Sur ce point, je dois être discret.

On parle beaucoup de cybercriminalité. La menace est-elle vraiment si forte ?

Au niveau mondial, le coût global de la cybercriminalité s'élève à 327 milliards d'euros et 77% des cyberattaques touchent des PME. En région Occitanie, 3 entreprises sur 4 ont déjà été victimes de piratage informatique. Et certaines ne s'en sont même pas rendues compte... Pourtant, en moyenne, 23 000 données sont volées par attaque : les virus récupèrent des données importantes et confidentielles des entreprises, comme les données financières mais aussi les données des clients. Les cyberattaques visent aussi les états.

Cette année, des cyberattaques spectaculaires ont eu un écho planétaire. Les virus sont-ils de plus en plus forts ?

Oui, ils progressent sans cesse. Pour preuve, on a vécu en 2017 des attaques de grande ampleur : les virus NotPetya et WannaCry ont causé des dégâts considérables dans le monde, paralysant des entreprises et des administrations. Ces virus sont des "ransomware", des logiciels qui infestent les machines pour prendre les données confidentielles en otage. Ils les cryptent pour les rendre illisibles : pour les récupérer, il faut payer... Justement, WannaCry s'est révélé être un virus particulièrement puissant d'un type nouveau : capable de combiner pour la première fois une attaque de masse et du phishing (usurpation d'identité, NDLR) de masse. Des entreprises paralysées ont dû payer.

A quels types de cibles ces virus peuvent-ils s'attaquer ?

A n'importe quel ordinateur. Avant WannaCry, les virus se contentaient de récupérer des données, ils n'avaient pas la puissance pour bloquer une entreprise. Aujourd'hui, ils peuvent bloquer des administrations entières, des états, et oui, bien sûr, des hôpitaux. Un virus peut désorganiser ou bloquer un hôpital, donner de fausses instructions, etc. On imagine les dégâts... Nous sommes dans le domaine de la cybercriminalité mais aussi du cyberterrorisme. Heureusement, l'impact des dernières attaques a placé le problème de la défense et de cybersécurité au premier plan. Et ce n'est pas du luxe...

Pourquoi ? Vous prévoyez une montée en puissance de la cybercriminalité ?

Malheureusement, oui. En janvier dernier, Ziwit a lancé une carte interactive de veille dans le monde des cyberattaques en temps réel. Cette carte nous a demandé de gros investissements, mais l'outil est extrêmement précieux, il scanne le web toutes les minutes, repère les cyberattaques et les identifie. On en recense 500 000 chaque jour sur la planète ! Cet outil nous permet de voir l'évolution de la cybercriminalité, ses armes, ses cibles, et d'en déterminer les tendances. Nous avons une idée précise de ce qui va arriver dans les six mois.

Et quelles bonnes nouvelles allez-vous nous donner ?

Pas si bonnes, malheureusement... Tout indique que nous allons vers une recrudescence des attaques de type ransomware, mais plus vraiment pour soustraire de l'argent aux victimes : plutôt pour du cybersabotage. Les virus vont tout simplement chercher à supprimer les données sans possibilité de les récupérer. C'est très grave... D'après nos prévisions, cette phase massive de cybersabotage va frapper avant la fin de l'année, et elle touchera tout le monde.

Les particuliers doivent-ils eux aussi se protéger ?

Bien sûr ! D'autant plus que le champ des cyberattaques va s'élargir avec la multiplication des objets connectés. Il y aura des attaques massives avec l'IoT. Nous avons dépassé le temps du pirate isolé, du geek cherchant surtout à relever un défi... Nous avons désormais affaire à des organisations

DOMAINE DE
VERCHANT
★★★★★ HOTEL & SPA

DOMAINE DE
VERCHANT
★★★★ HOTEL & SPA

criminelles capables de s'attaquer à de grandes entreprises ou des États. Il ne faut pas grand chose à un pirate pour rentrer dans un serveur : il peut y accéder par exemple à partir d'une caméra de surveillance, ou d'un frigo connecté. Les particuliers aussi peuvent en être victimes. Un conseil : faites régulièrement des sauvegardes sur des disques durs externes.

Outre adopter les solutions d'une entreprise comme la vôtre, y a-t-il d'autres solutions ?

Il faut contraindre les fabricants, de caméras ou de frigos par exemple, à sécuriser leurs systèmes pour empêcher les cyberpirates de remonter facilement jusqu'aux serveurs. La nouvelle loi européenne, la RGPD, doit permettre cette évolution. Il y a déjà eu des cas de hacking sur des voitures connectées, des modifications de paramètres dans des traitements d'e-santé, etc... Il faut bien comprendre qu'aujourd'hui, vos ordinateurs sont reliés à des systèmes, des serveurs par exemple, qui ne vous appartiennent pas... Il faut donc sécuriser toute la chaîne.

Vous pouvez répondre en urgence en cas d'attaque ? Trouvez-vous toujours la réponse ?

Nous avons mis en place un protocole, l'Incident Response team, qui permet de stopper à distance les actions menées par les hackers mais aussi de remédier aux dommages causés par les intrusions. Donc, oui, nous arrivons à apporter la bonne réponse. Pour cela, Ziwit investit constamment dans la R&D pour garder de l'avance. Notre technologie est difficile à reproduire. Nous avons recruté les meilleurs mathématiciens et les meilleurs cryptologues pour développer une sorte d'Intelligence Artificielle qui évolue et apprend depuis 6 ans. Cette avance, la concurrence ne peut pas la reproduire.

Dans ce genre de situation, la concurrence préfère acheter !

(rires) Nous avons eu des propositions, en effet, mais non, je ne vends pas. Je ne dépends d'aucun actionnaire, donc je suis libre. Je reste à Montpellier où il y a tout : l'écosystème numérique, la French Tech, la navette d'Air France, bientôt le nouveau TGV... Ici, comme je ne dois pas reverser d'argent à des actionnaires, je peux réinvestir massivement dans la R&D.

6 M€ pour le Fonds Stratinvest

La French Tech Montpellier est labellisée réseau thématique de #Security #Privacy, et Ziwit est sa pépite... La société de Mohammed Boumediane a lancé en juin Stratinvest, un fonds d'investissement doté de 6 M€ dédié aux projets de cybersécurité et de cyberdéfense. Le fonds, entièrement financé par Ziwit, entend soutenir des projets à hauteur de 500 000 à 1 M€. "Je me suis inspiré des deux références mondiales dans ce domaine : le fonds américain In-Q-Tel et le fonds israélien Libertad. Stratinvest doit nous permettre d'accompagner un ou deux projets d'ici à la fin de l'année", annonce le jeune dirigeant qui vise à terme une bonne dizaine de projets accompagnés. Selon lui, Montpellier doit jouer la carte de la cybersécurité : "Stratinvest doit se substituer aux fonds d'investissement traditionnels, assez peu réactifs aux projets de cybersécurité. En effet, tout ce qui touche à la défense fait peur aux investisseurs car il faut de gros efforts en R&D pour un marché, au final, assez difficile d'accès. Il faut un solide carnet d'adresses et beaucoup de réseau".Mohammed Boumediane dispose de l'un et de l'autre... Et, peut-être même, bientôt, de moyens renforcés avec l'arrivée d'un financeur, "un leader du secteur de la défense", assure le jeune dirigeant.

Mohammed Boumediane, en quelques lignes

Dès 14 ans, ce féru de mathématiques s'intéresse à l'informatique et participe à des challenges organisés par de grandes entreprises qui demandent à de jeunes talents du clavier d'essayer de craquer leurs systèmes. Il gagne 400 000 dollars à l'un de ces concours.

Il passe ensuite un bac en mathématiques et intègre le prestigieux Institut d'ingénierie informatique de Limoges. Après avoir travaillé dans de grandes sociétés du secteur de la défense, il s'installe à Montpellier, réputée comme une place forte de la cybersécurité en Europe, pour créer Ziwit, aujourd'hui installée dans la Mantilla, le quartier situé le long de l'avenue de la Mer.

A 30 ans, Mohammed Boumediane est devenu le dirigeant d'une société en passe de devenir le leader mondial de la cybersécurité et de la cyberdédense: "Nous ne sommes encore que le leader européen : nous ne sommes pas encore en Asie", s'amuse celui dont les solutions veillent à la sécurité informatique des pays de l'OTAN. Ziwit et ses 200 salariés dans le monde (dont une partie à Montpellier) réalise 70% de son activité à l'export, "notamment avec les services secrets américains".

DOMAINE DE
VERCHANT
★★★★★ HOTEL & SPA