ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE

Press Release

Des chercheurs obtiennent plus de 2 millions de dollars pour repenser la cybersécurité

Cyberhaven développe un nouveau concept de sécurité informatique. La spin-off de l'EPFL ouvre des bureaux à Boston et obtient plus de 2 millions de dollars d'investissements privés.

Les antivirus sont-ils définitivement hors course? C'est en tous cas l'opinion de George Candea, et il n'est pas le seul expert en sécurité informatique à le penser. "Dans les multinationales ou les agences gouvernementales, on utilise plus souvent les anti-virus par obligation légale, ou pour souscrire aux conditions des assureurs, que pour leur réelle efficacité", affirme-t-il. Avec ses anciens doctorants, le professeur de l'EPFL a fondé la start-up Cyberhaven, qui développe un tout nouveau concept de sécurité informatique. Avec des résultats prometteurs. Lors d'un récent test indépendant, leur solution a permis de détecter l'ensemble des 144 malwares - des logiciels malveillants - introduits par des hackers professionnels, tandis que les solutions modernes de sécurité, basées sur des méthodes dites "heuristiques", n'en dénichaient qu'une vingtaine. Quant au meilleur des antivirus classiques testés, il n'en trouvait qu'un seul. "Et encore, il a eu de la chance!", s'amuse le chercheur.

Depuis sa création début 2015, Cyberhaven a déjà pu générer 640'000 dollars de revenus. Des résultats plus qu'encourageants pour une jeune pousse, qui lui auront permis d'obtenir plus de 2 millions de dollars d'un premier tour de financement, de la part de la société américaine de capital risque Accomplice, l'une des plus actives aux USA dans le domaine des start-ups. Elle peut ainsi commencer son activité d'affaires à Boston et continuer de développer sa R&D en Suisse, au parc d'innovation de l'EPFL.

La solution de Cyberhaven s'adresse tout particulièrement aux grandes entreprises ou aux agences gouvernementales, qui font l'objet d'attaques sur mesure. Les pirates n'hésitent pas à développer des logiciels malveillant ad hoc pour atteindre ces cibles. Dans ce cas, les produits de sécurité les plus courants sont de peu d'utilité. On aligne des pare-feu les uns derrières les autres. "Cela va jusqu'au point où le chargé de la sécurité ne maîtrise plus l'ensemble du système, tant il a installé de solution différentes", témoigne George Candea.

Protéger les données au moment où elles sont décryptées

Les chercheurs de l'EPFL ont développé un concept de sécurité informatique totalement novateur et simple à déployer. Il complète l'outil le plus efficace à ce jour pour la sécurité, soit l'encryptage des fichiers, que de nombreux produits permettent. Par exemple, Microsoft Office comprend une option d'encryptage.

Mais l'encryptage seule ne suffit pas. Lorsqu'on ouvre un fichier ainsi protégé, par exemple un document texte, le programme doit le décrypter pour que l'utilisateur puisse accéder au contenu. Les données sont disponibles "en clair" sur la mémoire de la machine. C'est le moment que choisissent les pirates pour accéder aux données, souvent en détournant l'application elle-même, par exemple un traitement

de texte, qui leur ouvre les portes de tous les fichiers protégés auxquels il a accès. Dans l'entreprise, cela constitue le véritable talon d'Achille de la sécurité.

Le technologie de Cyberhaven protège les documents sensibles et le programme qui les exploite en créant autour d'eux un espace sécurisé. "Seuls les document analysés comme sûrs peuvent être admis dans cette zone. Notre méthode de protection n'a rien à voir avec les solutions basées sur l'heuristique, qui listent des activités inhabituelles. Notre programme analyse ce qui se passe instruction par instruction, il ne procède pas par suppositions." Cette méthode d'analyse a demandé plus de sept ans de recherche à l'EPFL. Elle est protégée par quatre brevets à l'EPFL, dont Cyberhaven détient la licence.

Laisser entrer les logiciels malveillants, pour mieux les neutraliser
Contrairement au pare-feu traditionnel, le logiciel de Cyberhaven ne bloque pas l'entrée aux malwares, mais il les empêche d'agir. "Plutôt que de construire une forteresse, de cumuler des dizaines de pare-feu, nous avons décidé de protéger des workflows indépendants, c'est à dire l'ensemble d'applications, de fichiers et d'utilisateurs impliqués dans une activité sensible donnée, par exemple la préparation d'un rapport financier ou la négociation d'un accord intergouvernemental. En combinant l'encryption et la solution de Cyberhaven, on peut se passer de nombre de solutions existantes pour une infratsructure plus simple et robuste."

"Il fallait nous installer aux USA pour continuer de travailler en Suisse"
Selon George Candea, il fallait une recherche académique pour oser aborder le problème de la sécurité en des termes nouveaux. "Parfois l'industrie peut rester bloquée sur d'anciens paradigmes. Je crois que seule une équipe de scientifiques pouvaient re-penser le problème depuis le début." Des scientifiques qui ont continué à développer leur idée. Cyberhaven est entièrement dirigée par d'anciens doctorants du laboratoire de George Candea à l'EPFL.

Pour l'heure, Cyberhaven compte huit employés en Suisse. L'un des co-fondateurs, Vova Kuznetsov, est maintenant chargé de développer les quartiers de l'entreprise à Boston. "La Suisse est forte d'une exceptionnelle densité de personnel qualifié et d'infrastructures de qualité, mais c'est aussi un très petit marché. En nous installant aux USA, nous nous donnons une chance de faire croître en Suisse notre recherche et développement, explique George Candea. Mais les Etats-Unis ne sont pas qu'un énorme marché, ils sont aussi l'opportunité de nous lancer dans une concurrence acharnée avec les meilleurs experts du monde entier."

Cyberhaven, les personnes clés: Dr. Vova Kuznetsov, CEO / Dr. George Candea, Chairman / Dr. Cristian Zamfir, COO / Dr. Radu Banabic, VP of Engineering / Dr. Vitaly Chipounov, Chief Architect

Contacts

- Lionel Pousaz, Service de presse de l'EPFL, lionel.pousaz@epfl.ch
  ou +41 79 559 71 61

- George Candea, chercheur EPFL, george.candea@epfl.ch
  ou +41 79 822 70 15