Researchers raise more than two million dollars to rethink cybersecurity

July 28 2016

Is antivirus software already dead? That's certainly what George Candea believes, and he's not the only computer security expert who says so. "Large enterprises and government agencies often deploy antivirus software to satisfy legal obligations or to meet contractual requirements, not because they really believe that the software can defend them," says George Candea. Together with some of his former PhD students, the EPFL professor founded Cyberhaven, a startup that is developing a brand new approach to computer security. And their results are promising. In a third party test, their solution warded off all 144 cyber attacks that had been hand-crafted by professional penetration testers, whereas so-called heuristic modern security products caught just over 20 of them. As for the best classical antivirus software tested, it only caught one. "I think it just got lucky!," muses the researcher.

Since it was founded in early 2015, Cyberhaven has had revenues of 640,000 dollars. This is encouraging for such a young company, and it enabled them to raise more than two million dollars in a first round of financing from Accomplice, one of the most active early-stage venture capital firms on the US East Coast. Cyberhaven will use the funds to set up its office in Boston and fuel the growth of its R&D team in Switzerland, at the EPFL Innovation Park.

Cyberhaven's solution is marketed mainly to enterprises and government agencies, which are all targets of sophisticated cyber attacks. Cyber criminals develop targeted malware that is unique to each of their attack campaigns. As a result, most of today's security products are not

effective against such new attacks. So organizations try to have defense perimeters within defense perimeters to build up so-called "defense in depth." "Information security officers eventually reach the point where their infrastructure is so complex that they simply cannot manage it anymore," says George Candea.

Defending "data in operation" against attack

The team of EPFL researchers developed a completely novel approach to defend sensitive documents against cyber attacks in a way that significantly simplifies an organization's security infrastructure. The approach complements what is perhaps the most effective security tool today, namely encryption - available in a wide variety of programs we use daily, including Microsoft Office.

Alas, encrypting documents is not enough to safeguard them. When opening an encrypted file, such as a text document, the application must first decrypt it in order to operate on it. As a result, the document's data is exposed. By exploiting vulnerabilities in applications like the Word text editor, malware hijacks them and steals all the documents that the application can access and decrypt. This is a real Achilles' heel of enterprise security, and encryption cannot solve it.

Cyberhaven's solution safeguards sensitive documents together with the relevant applications in a safe haven. "Only documents that are safe for these applications can enter the safe haven, and that also protects the integrity of the applications. Our defense technology is based on deep application analysis and has nothing to do with heuristics-based solutions that try to guess malicious behavior. We literally analyze every instruction, we never guess." Developing the technology took seven years of research at EPFL and is protected by four EPFL patents that have been licensed to Cyberhaven.

Neutralize malware instead of trying to keep it out

Unlike traditional defense techniques, Cyberhaven does not aim to keep all malware out of the enterprise but instead prevents it from acting. "Instead of building a fortress with many weak walls, we protect individual workflows that correspond to users' activities, such as the preparation of a quarterly financial report or the negotiation of a new inter-governmental agreement. By combining document encryption with Cyberhaven, it will no longer be necessary to use dozens of different security products to protect yourself; this will make your security infrastructure simpler and stronger."

"Expanding into the USA enables us to continue growing in Switzerland"

According to George Candea, fundamental academic research with novel perspectives is required to solve today's computer security problems. "Sometimes the industry can be stuck in a rut, so I believe it is up to researchers to rethink the problems from the ground up and come up with solutions." And, to fulfill their mission, this team of researchers is taking the execution of their vision in their own hands: Cyberhaven's leadership is entirely composed of former PhD students from George Candea's lab at EPFL.

Cyberhaven now has eight full-time employees in Switzerland. One of the co-founders, Vova Kuznetsov, has taken over the reins and is setting up the company's headquarters in Boston. "Switzerland has exceptional talent and quality infrastructure, but it is also a small market. By expanding into the US, we make it possible to grow our R&D in Switzerland, explains George Candea. And the US is not just a huge market, it is also an opportunity to compete with the very best, and that pushes us to become better."

Provided by Ecole Polytechnique Federale de Lausanne