PRESS RELEASE - PARIS – 7 DECEMBER 2021

Cybermallix counter-attack against viruses and malware

- Malware, or malicious software, pirates our data, destroys our software and hard drives, and forces our computers to pour forth torrents of spam. It is a major issue in cybersecurity today.
- The CNRS, l'Université de Lorraine, Inria, and the company WALLIX have joined forces to step up the fight against malware.

The CNRS, l'Université de Lorraine, Inria, and WALLIX, a European cybersecurity software publisher, have combined their skills to step up the fight against malware. The goal is to conceive and develop predictive cybersecurity solutions based on artificial intelligence in order to maximize the detection of malicious software. This partnership will become official on 7 December 2021 through the creation of a new associated research laboratory, Cybermallix.

"It is with great pride that we make our partnership with WALLIX official today. We are constantly pursuing our policy of developing associated research laboratories with companies of all sizes ranging from large groups to small and medium-sized companies as demonstrated by our more than 200 associated laboratories. This new associated laboratory will work on cybersecurity, an essential area for French industry, and more specifically on the use of AI in this field," enthuses CNRS CEO Antoine Petit. *"Malware is constantly evolving, and only artificial intelligence can provide a maximum level of security,"* stresses WALLIX CEO Jean-Noël de Galzain. "*This scientific collaboration is a considerable step forward in predictive cybersecurity,"* agrees Pierre Mutzenhardt, President of l'Université de Lorraine.

The Lorrain Research Laboratory in Computer Science and its Applications (LORIA, CNRS/Inria/Université de Lorraine) has for many years conducted research on cybersecurity. Thanks to its malware collection of over 30 million, researchers at LORIA'S High-Security Laboratory (the equivalent of a high-security laboratory in biology) conceive tools to combat computer viruses, such as solutions based on machine learning and formal methods[1] that can recognize the "morphology" of malware.

Thanks to its portfolio of unified solutions for securing access to data and digital identities, WALLIX can detect intrusions into a company's computer system in real time. The company now wants to offer additional protection that can anticipate cyberthreats. To do so, WALLIX and the research laboratory are jointly developing artificial intelligence technologies that are directly integrated in two of the company's solutions for securing accounts and workstations[2,3]. This collaboration will enable WALLIX to offer cutting-edge cybersecurity solutions.

Scientists from the CNRS, Inria and l'Université de Lorraine will also jointly conduct cybersecurity research with WALLIX engineers to explore security-related issues for connected objects, autonomous vehicles in

particular. They will also enhance the monitoring and detection of malicious code, especially through the use of machine learning and artificial intelligence.

Jean-Noël de GALZAIN, founder of WALLIX; Jean-Yves Marion, director of Loria; Jean-Luc MOULLET, deputy director general for innovation at CNRS; François Cuny, deputy director general for innovation at INRIA; Karl Tombre, University of Lorraine; Jean-Gabriel Kammerer, director - R&D Office at WALLIX © Emmeline Rousseau, CNRS

Notes

[1] Machine learning is a computer's capacity to "learn" from data, which is to say to improve its performance in performing tasks for which it was not explicitly programmed. Formal methods involve computing techniques that use specialized languages and logical rules to ensure there are no flaws in a computer programme.

[2] WALLIX Bastion manages, controls, supervises, and guarantees the traceability of privileged users while securing passwords for hardware and infrastructure applications.
[3] WALLIX BestSafe is based on a technology that applies the principle of least privilege to workstations. Regardless of profile—whether it is an administrator, manager, or collaborator—the user can only execute the limited computing tasks that were previously defined for that workstation. This drastically reduces the risk of intrusions and hence of cyberattacks.

Contact

CNRS press I Alexiane Agullo I **T +33 1 44 96 43 90** I alexiane.agullo@cnrs.fr