A3, un antivirus Open Source qui s'adapte à la menace

Des chercheurs de l'Université de l'Utah ont mis au point un logiciel capable non seulement de détecter, d'éliminer de nouveaux virus et malwares, mais aussi de réparer automatiquement les dommages occasionnés et d'immuniser l'ordinateur. Cette suite logicielle Open Source, baptisée A3 pour Advanced Adaptive Applications, embarquée dans une machine virtuelle, a été conçue pour surveiller l'OS (Linux pour les besoins du test) et les applications, explique Eric Eide, professeur assistant à l'Université de l'Utah en charge de ce projet. Ce dernier a été co-développé avec la firme **Raytheon BBN**, spécialisée dans la Défense et sous contrat avec le gouvernement américain. Le financement a été assuré par le programme « Clean-Slate Design of Resilient, Adaptive, Secure Hosts (CRASH) » de la **DARPA** (Defense Advanced Research Projects Agency). Ce programme d'une durée de 4 ans s'est achevé à la fin septembre.

A3 a été pensé pour protéger les serveurs et les stations de travail qui fonctionnent sous Linux. La suite a également été construite pour sécuriser les applications militaires. Il n'y a donc pas pour l'instant de plans pour adapter A3 aux PC ou notebooks personnels, souligne Eric Eide, « *mais cela pourrait être possible à l'avenir ; les terminaux pourront se protéger contre les malwares qui se propagent rapidement ou les corruptions des firmwares des composants* ».

Une multi-surveillance par plusieurs débogueurs

Concrètement, l'équipe de chercheurs a créé des « **débogueurs empilables** », c'est-à-dire plusieurs programmes de corrections d'erreur qui les uns après les autres surveillent constamment le comportement du système d'exploitation et des applications. Contrairement à un antivirus de PC qui compare les signatures de virus en fonction d'un catalogue, A3 s'appuie sur la **contextualisation** (comportement anormal de l'OS ou des applications) pour repérer des menaces inconnues. Dans ce cas-là, A3 peut bloquer le virus, réparer le code impacté et enfin apprendre à ne plus être infecté de nouveau par cette menace. Les scénarios d'usage sont évidents dans le cadre militaire pour assurer la continuité des applications, mais on peut imaginer qu'A3 puisse être utilisé par des services Web comme Amazon pour détecter, bloquer et réparer une attaque en quelques minutes sans avoir à arrêter les serveurs.

Pour tester l'efficacité de la solution, les chercheurs et Raytheon BBN ont fait une démonstration à la DARPA en se basant sur la faille ShellShock qui touche l'outil en ligne de commandes Bash et qui a fait beaucoup de dégâts chez les acteurs du web. « *A3 a découvert l'attaque via ShellShock sur un serveur web et réparé les dommages en 4 minutes* », précise Eric Eide. En parallèle, l'équipe a testé la suite avec une demi-douzaine d'autres malwares, avec succès. Maintenant que les tests ont validé la technologie, les scientifiques souhaitent perfectionner leur projet et trouver un moyen de l'utiliser en mode Cloud.

A lire aussi :
Des trous de sécurité trouvés dans 14 antivirus
Les entreprises françaises gardent la sécurité IT en interne