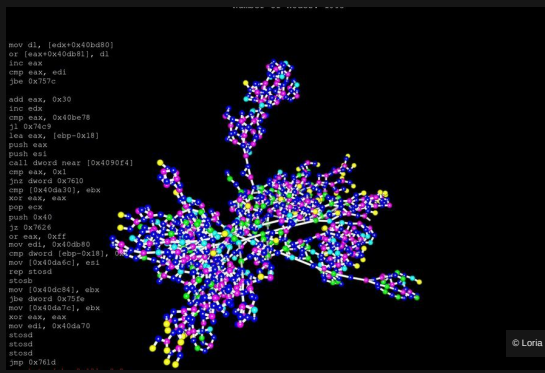
Cybersécurité : comment le Laboratoire de Haute Sécurité de Nancy analyse la morphologie des malwares pour mieux les détecter

Le Laboratoire lorrain de recherche en informatique et ses applications (Loria) abrite le Laboratoire de Haute Sécurité (LHS) à Nancy (Grand Est). Dans ce lieu sécurisé, les chercheurs étudient les logiciels malveillants (malwares) et analysent leur morphologie en vue de les détecter le plus tôt possible.

Abdessamad Attigui

27 octobre 2023 \ 10h00

3 min. de lecture



© Loria

Un malware étudié par le LHS.

Niché au cœur des locaux de l'INRIA et du Loria à Nancy, le Laboratoire de Haute Sécurité est le fer de lance de la recherche nationale en matière de cybersécurité. Depuis 2008, il s'est donné pour mission de lutter contre la prolifération de malwares, ces logiciels malveillants qui touchent les objets connectés (IoT) et les systèmes industriels (ICS/Scada). Le mercredi 25 octobre, Jean-Yves Marion, professeur à l'Université de Lorraine et chercheur au Loria, a présenté les avancées du laboratoire en la matière, notamment l'analyse morphologique, qualifiée de *« première mondiale »*.

Séparé des autres infrastructures du Loria, ce lieu clos traque, collecte et étudie des malwares de rançonnage (ransomwares) et leurs variants qui parviennent à échapper aux systèmes de protection existants en utilisant une technique d'obfuscation de code. *« Ils sont polymorphes et packés, c'est-à-dire que le fichier malveillant est caché, compressé jusqu'au moment de l'exécution »*, pointe Jean-Yves Marion.

Derrière la porte blindée, une petite pièce du LHS comporte deux éléments clés. Une salle de cluster équipée d'un « télescope virtuel » pour détecter les codes malveillants. Celui-ci surveille les vagues de cyberattaques en temps réel, permettant aux chercheurs d'observer des milliers d'attaques en direct. *« Par exemple, lors des élections américaines de 2016 ou pendant le conflit Ukraine-Russie, le télescope a enregistré des flots d'attaques sur les serveurs »*, commente le professeur.

Pour les intercepter et les collecter, le laboratoire dispose d'un « pot de miel virtuel », une ruse qui attire les cyberattaquants en leur faisant croire qu'ils ont trouvé la proie idéale. *« Ces deux infrastructures nous permettent d'analyser les malwares sans risquer de contaminer l'ensemble du réseau »*, souligne-t-il.

Caractériser les souches de virus existants

À ce jour, la base de données du LHS renferme 35 millions de malwares que les chercheurs ont minutieusement analysés pour développer une technique d'analyse dite morphologique, une avancée résultant de dix années de recherche fondamentale. Cette méthode repose sur un système d'intelligence artificielle, entraîné par apprentissage automatique, permettant d'identifier les fonctionnalités cachées dans les programmes tels que des applications et des mises à jour en se basant sur la forme du virus. Cela permet de détecter rapidement les intrusions qui échappent aux systèmes de détection existants.

Concrètement, l'approche implique de prendre en considération la structure globale d'un programme, de le désassembler, d'extraire des signatures - *« une sorte de souche de virus connu »* - et de le cartographier pour caractériser ses fonctionnalités. *« La recombinaison partielle de ces signatures permet de retrouver des similitudes entre le code analysé et un malware déjà identifié, ce qui facilite la détection des fonctionnalités indésirables dans un programme »*, souligne Jean-Yves Marion.

Le logiciel « Gorille » pour détecter des « variants »

La solution est commercialisée par la start-up Cyber-Detect, spin-off du Loria (CNRS, Inria, Université de Lorraine). Lancée en 2017, l'entreprise a transformé cet outil en une véritable arme contre les malwares à travers son logiciel « Gorille ». Avec l'analyse morphologique, il repère les dérivés des virus qui portent la même signature, avant qu'ils ne passent à l'attaque, selon la société. *« Comme en biologie, certains virus sont des mutants. Les cyberattaquants les font varier pour tromper les antivirus*, indique Régis Lhoste, son fondateur. *Nous pouvons ainsi repérer dans un virus des parts de LockBit, de DarkSide, de BlackMatter ou de ZLoader. »*

Selon les informations fournies par Cyber-Detect, ce logiciel affiche un taux de détection compris entre 95 % et 100 % pour les malwares connus, et de 90 % pour les variants. Cette solution est d'ores et déjà adoptée par des entreprises, dont Thales. Elle est utilisée pour des tâches variées, notamment l'analyse forensique visant à déterminer le mode opératoire et les conséquences post-attaque, la recherche de CVE (vulnérabilités et expositions courantes) ainsi que la vérification de l'intégrité des firmwares (mises à jour, nouvelles fonctionnalités d'un programme).

Par ailleurs, le LHS poursuit ses travaux avec en ligne de mire le développement de nouvelles approches d'analyse et de détection pour doter les *« industriels et les services étatiques de capacités d'anticipation et de réactions rapides face aux cyber-attaques »*, glisse Jean Yves Marion.