# Des trous de sécurité trouvés dans 14 antivirus

Il y a quelques mois, un dirigeant de Symantec avait expliqué que l'antivirus était mort. Une phrase aussitôt modérée en expliquant qu'un antivirus seul ne pouvait pas lutter efficacement contre les menaces. Le chercheur **Joxean Koret**, de la société Coesinc basée à Singapour, en rajoute une couche en concluant que la majorité des antivirus comporte des vulnérabilités plus ou moins importantes.

Sa démonstration a été faite lors de Syscan 360, une conférence sur la sécurité à Pékin au début du mois de juillet. Il a **passé au crible 17 antivirus et leurs moteurs** et a découvert des failles importantes dans 14 d'entre eux. Parmi les produits mis en avant, il y a Avast, Bitdefender, Avira, Panda, AVG, Comodo, ClamAV, DrWeb, ESET, F-Prot, F-Secure et eScan. Une mention spéciale est accordée pour les 4 premiers qui comprennent plusieurs failles locales et exploitables à distance importantes. Dans la plupart des cas, le chercheur a informé les éditeurs pour qu'ils corrigent les différents bugs trouvés. Il salue les initiatives de certains comme Avast qui a un programme (Bug Bounty) pour traquer les vulnérabilités.

Cependant, Joxean Koret développe son analyse et pointe du doigt les différentes faiblesses des antivirus. Leur installation accorde **des privilèges administrateurs aux utilisateurs** et les pilotes accèdent au noyau du système d'exploitation. Il poursuit en expliquant que les mises à jour des produits ne sont pas signées et leur téléchargement s'effectue en http. Une attaque de type Man in the Middle peut dès lors être possible en HTTPS et donner la possibilité aux attaquants de prendre le contrôle des machines.

## Une surface d'attaque plus importante pour les entreprises

Par ailleurs, la majorité des antivirus sont codés en C, un langage jugé obsolète par l'expert et soumis à des attaques en corruption de mémoire (débordement de tampon mémoire). Il constate aussi que la plupart des antivirus embarquent certes des mesures défensives comme ASLR (Address Space Layout Randomisation), mais d'autres fonctions comme DEP (Data Execution Prevention) pour empêcher l'exécution de code se retrouvent parfois désactivées ou invisibles pour l'utilisateur.

En conséquence, Joxean Koret souligne que « *si ces applications s'exécutent avec des privilèges les plus élevés, installe des pilotes dans le noyau de l'OS, filtre les paquets et gère tout ce qu'un ordinateur doit faire, la surface d'attaque augmente de manière spectaculaire* ». Dans sa présentation, il donne quelques pistes de réflexion pour améliorer la sécurité des antivirus, comme de faire tourner du code jugé dangereux dans un émulateur ou une machine virtuelle. Il préconise aussi l'audit des antivirus sur le code des moteurs, ainsi qu'en utilisant le fuzzing, un test de données aléatoires pour vérifier les logiciels. Il rappelle de ne pas utiliser les élévations de privilèges pour scanner des paquets ou vérifier des fichiers. Il conclut en s'interrogeant : « *Pourquoi est-il plus difficile de mener des exploits sur*

*les navigateurs que sur les produits de sécurité ?* **»**

**A lire aussi :**
L’ère des antivirus arrive-t-elle à son terme ?
DAVFI : l’antivirus souverain s’appellera Uhuru