La NSA va publier le code d'un outil de reverse engineering de logiciels

La NSA (National Security Agency) va rendre disponible en open source un outil de reverse engineering répondant au nom de GHIDRA.

Un outil de reverse engineering de logiciels

L'organisme gouvernemental du département de la Défense des États-Unis publiera gratuitement cet outil à l'occasion de la prochaine conférence sur la sécurité de la RSA qui se tiendra début mars à San Francisco.

Baptisé GHIDRA, il s'agit d'un désassembleur, c'est-à-dire un logiciel qui décompose les fichiers exécutables en un code d'assemblage pouvant ensuite être analysé par des personnes.

Développé au début des années 2000, la NSA avait commencé à le partager depuis plusieurs années avec d'autres agences gouvernementales américaines luttant contre les cyber-menaces.

La CIA y avait notamment eu accès, comme l'avait montré Wikileaks en publiant Vault7, une quantité massive de fichiers internes dérobés sur l'intranet (réseau interne) de la Central Intelligence Agency.

La NSA déjà adepte de l'open source

Codé en Java, GHIDRA est doté d'une interface utilisateur graphique qui fonctionné sous différents OS (Windows, Linux et macOS).

Holger Mueller de Constellation Research estime que « la NSA souhaite exploiter les avantages clés de l'open source, qui consistent en un nombre accru de regards et de mains sur un ensemble de codes ». Quant aux outils de reverse engineering, « ils sont essentiels pour évaluer la propreté des logiciels vis-à-vis des logiciels malveillants. Avec de plus en plus d'affaires dépendant de logiciels, toutes les parties doivent disposer de bons outils pour valider les logiciels. "

La NSA n'en est pas à son galop d'essai dans l'open source. L'agence américaine dispose en effet une page GitHub répertoriant pas moins de 32 projets.