MEDIAPART
LE JOURNAL LE CLUB

NUMÉRIQUE
31 mars 2017
Par Jérôme Hourdeaux

WikiLeaks publie l'outil permettant à la CIA de dissimuler ses attaques

"Marble" est un système utilisé par la CIA pour modifier le code source de ses virus informatiques afin de dissimuler leur origine, voire de les attribuer à un tiers. WikiLeaks publie son code source, ce qui pourrait permettre de démasquer des attaques qu'aurait menées l'agence américaine.

WikiLeaks a publié, vendredi 30 mars, le code source du "système Marble", un outil utilisé par la CIA pour masquer l'origine des attaques informatiques qu'elle peut mener. L'existence et les principes de fonctionnement du système Marble (Marble Framework en anglais) avaient déjà été révélés par WikiLeaks le 7 mars dernier lors de la première publication de "Vault 7", une série de documents dévoilant les outils d'espionnage de la CIA que l'organisation de Julian Assange détaille depuis peu à peu.

Selon une présentation de la CIA,

> "le Marble Framework est conçu pour permettre une offuscation [c'est-à-dire une dissimulation – ndlr] flexible et facile à utiliser lors du développement d'outils".

Lors d'une attaque informatique, l'un des enjeux est en effet de dissimuler ses traces. Pour cela, son auteur, qu'il soit une agence gouvernementale ou un hacker, tente le plus souvent d'effacer tout élément permettant de remonter à lui, que ce soit des traces de géolocalisation ou encore des éléments dans le code du logiciel ou du virus permettant de deviner sa nationalité, sa langue, son appartenance à un groupe…

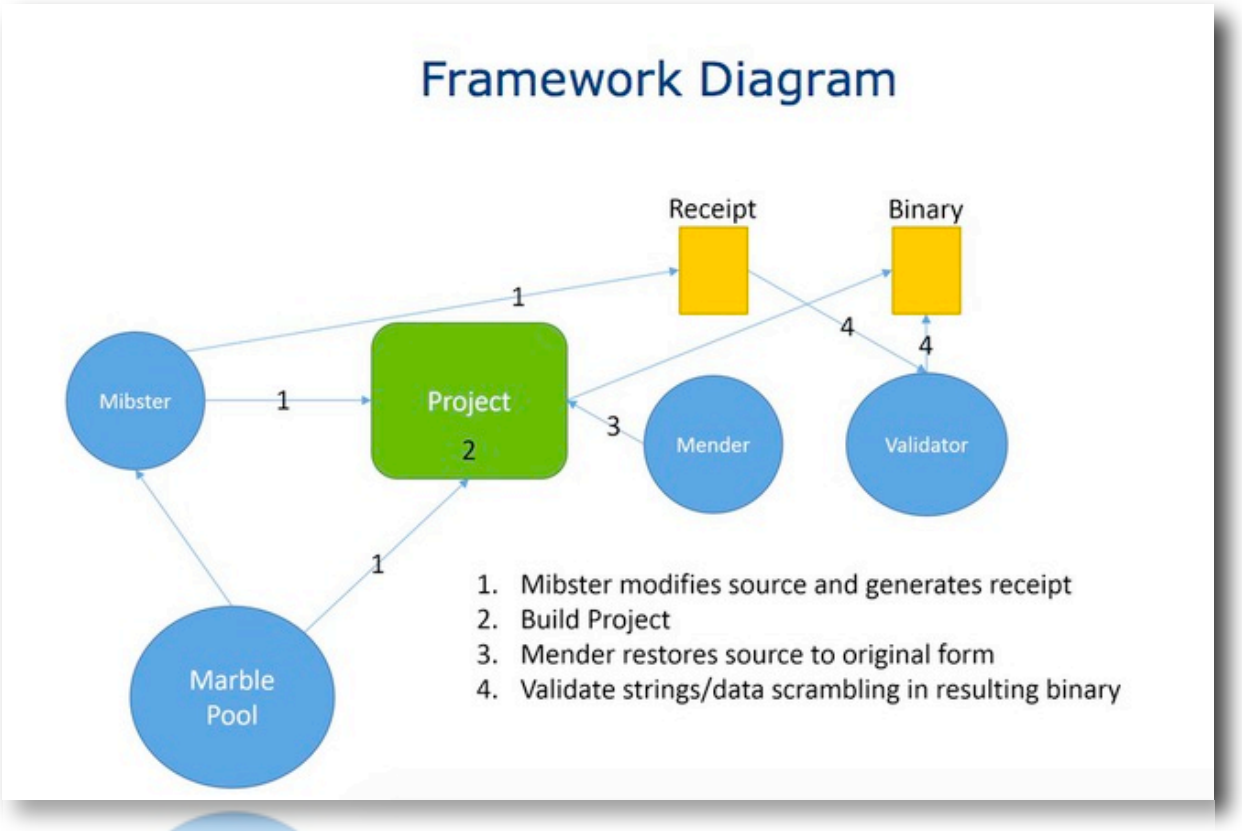
Dans l'idéal, l'attaquant essayera même de laisser des fausses pistes, des éléments laissant penser que l'opération a été menée par quelqu'un d'autre. Comme l'explique la présentation de la CIA, les outils d'offuscation

> "sont souvent utilisés pour lier un malware à un développeur ou à une équipe de développement spécifique" en modifiant le code source lui-même afin d'y insérer de fausses informations.

Ces méthodes rendent la question de l'attribution d'une cyber-attaque très délicate. Il faut bien souvent plusieurs mois voire années d'enquêtes et d'analyses pour parvenir à attribuer, avec seulement un certain degré de certitude, une attaque bien menée. Correctement réalisée, l'offuscation peut rendre une attaque intraçable, et conduire à la mise en cause d'un tiers.

Dans les grandes affaires récentes de piratages, les attributions de celui de Sony en 2014 à la Corée du Nord ou celui du Parti démocrate américain à la Russie font encore débat parmi les experts.

Encore récemment, au mois de février dernier, des chercheurs de la société de sécurité britannique BAE Systems travaillant sur "Lazarus", un virus qui s'est attaqué aux institutions financières d'une trentaine de pays, ont révélé que ses auteurs avaient volontairement introduit des termes russes dans son code source afin de brouiller les pistes.



WikiLeaks

Le système Marble permet à la Division d'ingénierie avancée (AED) de la CIA, chargée de développer ces outils, d'améliorer leurs méthodes d'offuscation en les automatisant. Les documents publiés début mars par WikiLeaks détaillaient ensuite la manière dont le Marble Framework est intégré dans le travail des ingénieurs de la CIA et ses différentes fonctionnalités.

La principale information de la publication de ce vendredi 30 mars est donc la publication du code source du Marble Framework, c'est-à-dire l'ensemble du texte comprenant toutes les instructions du programme, tel qu'écrit par ses concepteurs. Il s'agit en quelque sorte de l'ADN du système Marble qui se trouve ainsi dévoilé.

La publication d'un code source peut sembler d'un intérêt très limité pour le grand public. Celui-ci contient cependant potentiellement certaines informations d'une importance capitale pour les experts en analyse informatique et sa publication pourrait avoir de nombreuses conséquences.

WikiLeaks souligne ainsi que

"le code source du Marble Framework contient également un 'dé-obfuscator' ", une fonctionnalité permettant d'inverser l'offuscation mise en place par la CIA.

Celle-ci pourrait aider les chercheurs à faire émerger des "modèles ou des signatures" permettant de démasquer d'éventuelles attaques menées par l'agence, mais attribuées à d'autres.

"Le code source montre que Marble a des exemples tests pas seulement en anglais mais également en chinois, russe, coréen, arabe et farsi", souligne WikiLeaks.

Lire aussi

- WikiLeaks dévoile la "boîte à outils" de la CIA pour pirater vos appareils, Jérôme Hourdeaux
- Les élections françaises de 2012 étaient sous surveillance de la CIA, Jérôme Hourdeaux
- Des "cyber-armes" de la NSA sont mises aux enchères sur Internet, Jérôme Hourdeaux
- Dossier: la France et l'Allemagne sur écoute, La rédaction de Mediapart