Marble Framework

31 March, 2017

Today, March 31st 2017, WikiLeaks releases Vault 7 "Marble" -- 676 source code files for the CIA's secret anti-forensic Marble Framework. Marble is used to hamper forensic investigators and anti-virus companies from attributing viruses, trojans and hacking attacks to the CIA.

Marble does this by hiding ("obfuscating") text fragments used in CIA malware from visual inspection. This is the digital equivallent of a specalized CIA tool to place covers over the english language text on U.S. produced weapons systems before giving them to insurgents secretly backed by the CIA.

Marble forms part of the CIA's anti-forensics approach and the CIA's Core Library of malware code. It is "*[D]esigned to allow for flexible and easy-to-use obfuscation*" as "*string obfuscation algorithms (especially those that are unique) are often used to link malware to a specific developer or development shop.*"

The Marble source code also includes a *deobfuscator* to reverse CIA text obfuscation. Combined with the revealed obfuscation techniques, a pattern or signature emerges which can assist forensic investigators attribute previous hacking attacks and viruses to the CIA. Marble was in use at the CIA during 2016. It reached 1.0 in 2015.

The source code shows that Marble has test examples not just in English but also in Chinese, Russian, Korean, Arabic and Farsi. This would permit a forensic attribution double game, for example by pretending that the spoken language of the malware creator was not American English, but Chinese, but then showing attempts to conceal the use of Chinese, drawing forensic investigators even more strongly to the wrong conclusion, --- but there are other possibilities, such as hiding fake error messages.

The Marble Framework is used for obfuscation only and does not contain any vulnerabilties or exploits by itself.