#Vault7: WikiLeaks reveals ‘Marble’ tool could mask CIA hacks with Russian, Chinese, Arabic

31/03/2017

WikiLeaks’ latest batch of documents, named ‘Marble’, details CIA hacking tactics and how they can hamper forensic investigators from attributing viruses, trojans and hacking attacks to the spy agency . The tool was in use as recently as 2016.

Trends WikiLeaks CIA files

The third release, which contains 676 source code files for the agency’s secret anti-forensics framework, is part of the CIA’s Core Library of malware, according to a statement from WikiLeaks.

@**wikileaks** RELEASE: CIA Vault 7 part 3 "Marble" https://wikileaks.org/vault7/?marble#Marble%20Framework… #**Vault7**

> 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.*"

WikiLeaks said Marble hides fragments of texts that would allow for the author of the malware to be identified, meaning the agency allows another party to be blamed for the hack.

A Marble framework document reveals it supports the ability to *"add foreign languages"* to malware. *"Now comes the fun stuff,"* it reads, listing Chinese, Russian, Korean, Arabic and Farsi in example code, indicating the potential for the CIA to divert attention to international actors.

@_ChrisMaguire Within @wikileaks #Vault7 #Marble release, instructions on adding foreign language to algorithms to hide #CIA malware & hacks #dnchack

It's *"designed to allow for flexible and easy-to-use obfuscation"* as *"string obfuscation algorithms"* often link malware to a specific developer, according to the whistleblowing site.

READ MORE: #Vault7: How CIA steals hacking fingerprints from Russia & others to cover its tracks

"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," WikiLeaks explains, *"But there are other possibilities, such as hiding fake error messages."*

The code also contains a 'deobfuscator' which allows the CIA text obfuscation to be reversed. *"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."*

Previous Vault7 releases have referred to the CIA's ability to mask its hacking fingerprints.

WikiLeaks claims the latest release will allow for thousands of viruses and hacking attacks to be attributed to the CIA.