WikiLeaks: How the CIA Disguises Its Hacking to Appear to Be Foreign

Friday morning, WikiLeaks released the third of its “Vault 7” data and document dumps related to CIA hacking.

This latest drop, codenamed “Marble,” features 676 source code files for the CIA’s secret anti-forensic Marble Framework, which was used to hamper forensic investigators and anti-virus companies from attributing viruses, Trojans and hacking attacks to the CIA. It did this by hiding fragments of text used in its malware from visual inspection.

“This is the digital equivalent of a specialized CIA tool to place covers over the English-language text on weapons systems before giving them to insurgents secretly backed by the CIA,” the anti-secrecy group stated in a press release announcing the drop. “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 claims the Marble source code also includes a “deobfuscator” to reverse the hidden text. This, along with other revealed techniques, patterns and signatures, can be used by forensic investigators to correctly attribute previous hacking attacks and viruses to the CIA.

According to the group’s statement, the U.S. spy agency can make the attacks appear to be Russian, Chinese, North Korean, Saudi Arabian or Iranian.

“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," it stated. "The Marble Framework is used for obfuscation only and does not contain any vulnerabilties or exploits by itself."

This latest release follows the group's second release, codenamed "Dark Matter," by a little more than a week. In that statement, the group exposed how the CIA has infected Apple Mac firmware used on both computers and smartphones since at least 2008. {eoa}