New American

Written by **C. Mitchell Shaw** on April 1, 2017

CIA Has Tools for Framing Russia, China, Others for Hacks

The most recent release by WikiLeaks shows that the CIA has developed obfuscation tools for causing its hacks to be falsely attributed to foreign powers. And WikiLeaks has released not only the documents, but also the source code of those tools.

The third batch of "Vault 7" leaks — published by WikiLeaks Friday — show documented evidence that the CIA developed methods for obfuscating hacks and making it appear that the hacker was from Russia, China, North Korea, or Iran. The 676 files — code-named "Marble" — will certainly cast a shadow of doubt over claims from the past few years that certain hacks could be attributed to hackers in those countries.

According to a WikiLeaks press release:

> 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.

Since computer forensics — like other branches of forensic science — depends on finding and analyzing clues, Marble "plants" false clues sure to be spotted by investigators and helps removes clues that would lead those investigators to accurately attribute the real source of the hack. The end result is that the computer forensicists believe they have "proof" that the hacker was foreign (for instance, Russian). And because the "traces" of the hacking tools (deliberately) left behind indicate tools too advanced to have been developed without a government-sized budget, the next leap is that the hacker was state-sponsored. At least that part is true; but he works for the CIA, not the SVR or FSB.

Interestingly, WikiLeaks didn't just leak documents about the methods the CIA used, but has actually published the computer source code itself. WikiLeaks — having previously redacted documents and files in the Vault 7 leaks because of the dangerous nature of the cyberweapons involved — was careful to point out in this press release that "the Marble Framework is used for obfuscation only and does not contain any vulnerabilities or exploits by itself."

While this publication by the anti-secrecy website "does not contain any vulnerabilities or exploits," what it does contain is explosive. The source code the CIA used to obfuscate its hacking activities is laid bare for all to download, see, and examine. Wrapped up (or, technically, *zipped up*) in one nice little package of six folders containing 676 files, the source code is a smoking gun. The size of this particular package is deceiving. The whole package is only 539.8 kB in size. By way of comparison, the last picture this writer took on his OnePlus 3 smartphone was 32.58 mB (or more than 60 times larger than this entire leak).

But, if a picture is worth a thousand words, a line of computer code is worth the Library of Congress. And these particular lines of computer code serve as irrefutable evidence that the CIA has created a way to perpetrate fell deeds and frame other foreign powers for them.

As the press release says:

> 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."

And:

> 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.

While these files prove that the CIA created these tools for the purpose of making its hacking appear to have been perpetrated by state-sponsored hackers from Russia, China, North Korea, or Iran, they do not prove that the CIA ever actually used them for that purpose. Proving that is beyond the scope of the files published by WikiLeaks. Having said that, it seems beyond belief that the CIA would create (and continue to update) tools it never used for their intended purpose. If nothing else, the files certainly show intent; if they don't, then anyone ever arrested and charged with possession of burglary tools is owed an apology.

By creating these tools (and the documentation on the use of them), the CIA has turned computer forensics against itself. It is more than a little like a forensic technician doubling as a murderer and using his knowledge of forensics to cover his tracks. But this debacle by the CIA is a double-edged sword. Now that WikiLeaks has essentially "open-sourced" the CIA's code, there is a very real shadow of doubt hanging over every case where computer forensicists have positively attributed hacks to foreign powers. One now has to wonder if it the CIA might have perpetrated those hacks, or if it might have been someone else who gained access to the obfuscation tools developed by the CIA.

Some cases over just the last few years immediately come to mind.

• In late 2014, it was reported that a computer network at the White House had been hacked and that Washington had not even discovered the hack; an "ally" made U.S. officials aware of it. The evidence — including traces of computer code left behind — pointed to Russian state-sponsored hackers.

• Almost as soon as that story broke, reports of a cyberattack on America's infrastructure began

pouring forth. A complex Trojan Horse malware program, dubbed "BlackEnergy," was found to have infected critical government and industry networks including those that control vital parts of the nation's infrastructure — "complex industrial operations like oil and gas pipelines, power transmission grids, water distribution and filtration systems, wind turbines and even some nuclear plants." Again, the computer forensic evidence pointed to Russian state-sponsored hackers.

• In December 2014, Sony Pictures Entertainment was hacked to the tune of 100 terabytes of sensitive company data — including the full files of movies that had not even been released. All of that data was dumped to the Web. The FBI claimed that computer forensics pointed the finger squarely at North Korea — despite the fact that the Hermit Kingdom can't even keep the lights on in half the country at one time.

• In January 2015, ISIS reportedly hacked the Twitter and YouTube accounts for the U.S. military Central Command as well as the Twitter accounts and website servers of the *Albuquerque Journal* newspaper in New Mexico and WBOC 16 TV in Salisbury, Maryland. The hackers then posted anti-American, pro-Jihad videos and messages.

• In June 2015, reports of the granddaddy of all hacks against the United States dominated the news cycle. The United States Office of Personnel Management (OPM) had its outdated security protocols laid to waste by hackers who then exfiltrated the personal data of more than 22 million Americans. This time, the traces of computer code and other computer forensic evidence pointed to China.

While all of these hacks (with the exception of the Sony hack) may have been exactly what they appeared to be, this new revelation from WikiLeaks indicates that it is possible they weren't. This writer — who wrote all of the stories linked above — would certainly take each of them with a grain of salt if he were reporting on them today. Because it is is no stretch of the imagination to think that the CIA could have orchestrated any or all of them for the purpose of fomenting aggression toward the nations who were blamed. It is also possible that hackers who gained access to the CIA's tools used them for what they were made for — covering their tracks.

Regardless of whether these hacks were carried out by foreign powers, the FBI, or teenagers, the one thing that is certain is that the intelligence community cannot be trusted.