CIA Develops Undetectable Implants on Windows Computers: WikiLeaks

01/09/2017

"Like previously published CIA projects (Grasshopper and AfterMidnight) in the Vault 7 series, it is a persistent framework that can load and execute custom implants on target computers running the Microsoft Windows operating system (XP or Win7)," the WikiLeaks statement said.

According to a leaked CIA manual, the tool is called "Angelfire" and consists of five components: Solartime, Wolfcreek, Keystone (previously MagicWand), BadMFS and the Windows Transitory File system. Each has its own functions.

After Angelfire is installed on a computer, Solartime modifies the partition boot sector of the Windows XP or Windows 7 machine, paving the way for Wolfcreek to load and execute the remaining implants.

As part of the Wolfcreek implant, Keystone then starts malicious user applications on the targeted computers, which reportedly never touch the file system.

“So there is very little forensic evidence that the process was ever ran,” WikiLeaks said.

BadMFS is described as a library that stores all drivers and implants that Wolfcreek can activate. It is created at the end of the active partition. It can be detected in some versions, but in most it’s encrypted and obfuscated.

Additionally, Windows Transitory File System is a newer component that is used to install AngelFire while adding and removing files from it.

The Angelfire framework is just another tool in the CIA's arsenal for hacking Windows users. Since March, WikiLeaks has released details on CIA hacking tools in its Vault 7 series, which contained a total of 8,761 documents.

WikiLeaks said the leaked documents came from within the CIA, which has in turn refused to confirm their authenticity.