CIA sneak undetectable ‘malicious’ implants onto Windows OS - WikiLeaks

31/08/2017

Windows machines are targeted by the CIA under ‘Angelfire,’ according to the latest release from WikiLeaks’ ‘Vault7’ series. The documents detail an implant that can allow Windows machines to create undetectable libraries.

‘Angelfire’ consists of five components – ‘Solartime,’‘Wolfcreek,’ ‘Keystone,’ ‘BadMFS,’ and the ‘Windows Transitory File system,’ according to a statement from WikiLeaks released on Thursday.

‘Solartime’ modifies the partition boot sector of Windows XP or Windows 7 machines when installed, allowing the ‘Wolfcreek’ implant to load and execute. ‘Wolfcreek’ can then load and execute other ‘Angelfire’ implants.

Previously known as ‘MagicWand,’ ‘Keystone’ loads malicious user applications on the machine which never touch the file system, leaving *“very little forensic evidence that the process ever ran”* according to WikiLeaks.

@RT_com #Vault7: CIA can intercept & redirect SMS on Android, according to #Highrise document https://on.rt.com/8hpp

‘BadMFS’ is described as a library which stores all drivers and implants that ‘Wolfcreek’ can activate. In some versions it can be detected, but in most it’s encrypted and obfuscated, making it undetectable to string or PE header scanning, used to detect malware.

‘Windows Transitory File system’ is used to install ‘AngelFire,’ according to the release, allowing the addition or removal of files from it.

WikiLeaks says the leaked ‘Vault 7’ documents came from within the CIA, which has in turn refused to confirm their authenticity. Previous releases include details on CIA hacking tools used to weaponize mobile phones, compromize smart TVs and the ability to trojan the Apple OS.

READ MORE: How the CIA spies on your everyday life, according to WikiLeaks