‘CIA’s Cherry Bomb’: WikiLeaks #Vault7 reveals wireless network targets

16/06/2017

The latest Wikileaks Vault7 release reveals details of the CIA’s alleged Cherry Blossom project, a scheme that uses wireless devices to access users’ internet activity.

The Cherry Blossom program also provides a means to perform software exploits on particular ‘targets’, meaning the hacker can take advantage of vulnerabilities on the target’s device, according to a Wikileaks press release.

Wikileaks notes that the common use of WiFi devices in homes, offices, and public spaces makes them ideal for these so-called ‘Man-In-The-Middle’ attacks as the Cherry Blossom program can easily monitor, control and manipulate the Internet traffic of connected users.

Malicious content can be injected into the data stream between the user and the internet service, which exploits vulnerabilities in the target’s computer or operating system, according to WikiLeaks.

No physical access is required to implant the customized Cherry Blossom firmware on a wireless device as some devices allow their firmware to be upgraded over a wireless link.

The new firmware on the device can be triggered to turn the router or access point into a so-called ‘FlyTrap’. The FlyTrap can scan for “email addresses, chat usernames, MAC addresses and VoIP numbers” in passing network traffic, according to the leaked documents.