1100 - Weaponizing the BBC Micro:Bit

Friday at 11:00 in Track 2

45 minutes | Demo, Tool, Exploit

Damien "virtualabs" Cauquil*Senior security researcher, Econocom Digital Security*

In 2015, BBC sponsored Micro:Bit was launched and offered to one million students in the United Kingdom to teach them how to code. This device is affordable and have a lot of features and can be programmed in Python rather than C++ like the Arduino. When we discovered this initiative in 2016, we quickly thought it was possible to turn this tiny device into some kind of super-duper portable wireless attack tool, as it is based on a well-known 2.4GHz RF chip produced by Nordic Semiconductor.

It took us a few months to hack into the Micro:Bit firmware and turn it into a powerful attack tool able to sniff keystrokes from wireless keyboards or to hijack and take complete control of quadcopters during flight. We also developed many tools allowing security researchers to interact with proprietary 2.4GHz protocols, such as an improved sniffer inspired by the mousejack tools designed by Bastille. We will release the source code of our firmware and related tools during the conference.

The Micro:Bit will become a nifty platform to create portable RF attack tools and ease the life of security researchers dealing with 2.4GHz protocols !

Damien "virtualabs" Cauquil

Damien Cauquil is a senior security researcher at Digital Security (CERT-UBIK), a French security company focused on IoT and related ground breaking technologies. He spoke at various international security conferences including Chaos Communication Camp, Hack.lu,Hack In Paris and a dozen times at the Nuit du Hack (one of the oldest French security conferences).

@virtualabs, https://www.digitalsecurity.fr

#defcon25/by_track/track2/friday   #defcon25/By_Day/_Friday