THE IMPACT OF TORII ON ARM ARCHITECTURE

Milorad Murić[1]; Žarko Bogićević[2];

[1] High school of vocational studies, Užice, Serbia, muricmilorad@gmail.com

[2] Technical school, Užice, Serbia, zarko1993@hotmail.com

***Abstract*:** *Already at the end of 2016, there are suspicions of the active operation of various botnet malware, of which the most famous are Mirai and Qbot. At a time when millions of different IoT devices are in use, the operation of such malware can be extremely dangerous. In the light of such developments, a new malware called Torii, which was detected at the end of September 2018, emerged. This brand new strain of malware strives to remain deeply hidden, acting persistently from the background and still does not take steps that are characteristic of most botnets . What's clear is that this malware can attack a wide range of different hardware-targeted architectures, such as MIPS, ARM, x86, x64, PowerPC, SuperH and others. The paper will explain how this malware works and the consequences it can cause, as well as the way we can protect itself and devices.*

Keywords : *Malware, Botnet,Torii, ARM*