Analyzing a Backdoor/Bot for the MIPS Platform

By Created by:Muhammad Junaid Bohio

Malware functionalities have been evolving and so are their target platforms and architectures. Non-PC appliances of different architectures have not traditionally been frequent targets of malware. However, many of those appliances, due to their enhanced processing power and/or low maintenance, provide ideal targets for malware. Moreover, due to the lack of security for home routers, they often remain infected until replaced, thereby providing longer persistence for a malware. Recently, there has been a surge in malware for the MIPS and ARM architectures, targeting specific routers, DVRs, and other appliances. These network devices, in comparison, get less focus from vulnerability researchers and firmware patch application by end-users. This increases the risk of compromise and requires additional skills to cope with malware exploiting these platforms. This paper discusses various tools and techniques for reversing malware for the MIPS platform. We perform static and dynamic analysis of a MIPS malware, discuss its Command and Control mechanism, and provide detection of its network communication.
