7.15 The negative impact of Malware and Attack Rootkits on the Forensic Memory Analysis

Hadia Hamid ¹, Izzeldin Amin ², Mohamed Khalil ³

¹Faculty of Mathematical Sciences, University of Khartoum, Sudan; hadiahamid@uofk.edu

Keywords: Memory forensics, Memory Analysis, Malware, Rootkits, malware detection techniques, rootkits detection techniques

When society becomes very dependent on technological assistants, it might be viewed as unsleeping witnesses. An important part on these assistants is its volatile data storage, because it may contain very useful data for the support or refute of a theory of how an offense occurred. If these data extracted using a memory forensics technique that put a considerable effort on extracting every single bit as much as possible in a forensically sound manner, this data might be admissible to the court and serve the crime. Memory forensics is a relatively recent field but it is growing and evolving rapidly, but it is attracting a considerable attention of the researchers from both industrial and academic sectors. However in most of the past and recent researches the negative impacts of the malware and attack rootkits is mostly overlooked, in spite the fact that it might hinder or impede the access to the artifacts through hide some objects intentionally, which could serve as a digital evidence that may condemns or exonerates the accused in a crime. This paper investigates the negative impacts of the malware and attack rootkits existence in memory while conducting a digital investigation. It also presents a wide range of malware and attack rootkits detection techniques, focusing on the hidden objects detection techniques. The main finding of this paper is drawing the attention of the researchers to the negative impacts of these malware and attack rootkits and the critical consequences of these impacts on the digital investigation process.