World Academy of Science, Engineering and Technology
International Journal of Cognitive and Language Sciences
Vol:11, No:10, 2017

The Proactive Approach of Digital Forensics Methodology against Targeted Attack Malware

Authors : Mohamed Fadzlee Sulaiman, Mohd Zabri Adil Talib, Aswami Fadillah Mohd Ariffin

Abstract : Each individual organization has their own mechanism to build up cyber defense capability in protecting their information infrastructures from data breaches and cyber espionage. But, we can not deny the possibility of failing to detect and stop cyber attacks especially for those targeting credential information and intellectual property (IP). In this paper, we would like to share the modern approach of effective digital forensic methodology in order to identify the artifacts in tracing the trails of evidence while mitigating the infection from the target machine/s. This proposed approach will suit the digital forensic investigation to be conducted while resuming the business critical operation after mitigating the infection and minimizing the risk from the identified attack to transpire. Therefore, traditional digital forensics methodology has to be improvised to be proactive which not only focusing to discover the root caused and the threat actor but to develop the relevant mitigation plan in order to prevent from the same attack.

Keywords : digital forensic, detection, eradication, targeted attack, malware
Conference Title : ICFSDF 2017 : International Conference on Forensic Sciences and Digital Forensics
Conference Location : Osaka, Japan
Conference Dates : October 09-10, 2017