2019

Existing Evidence for the Effectiveness of Honeypots in Preventing Cyber Crime Incidents

David Maimon
Georgia State University, dmaimon@gsu.edu

Existing Evidence for the Effectiveness of Honeypots in Preventing Cyber Crime Incidents

David Maimon
Center for Evidence Based Cybersecurity
Georgia State University

A honeypot is a technical tool that simulates a real computer system and permits the collection of information on hackers and real system trespassing events. Importantly, since honeypots have no production value (i.e. no legitimate users of the computer networks should use them), any network activity they initiate or receive means that the system has been compromised, and that system trespassers are using it for their own malicious operations. Information Technology managers use honeypots for the detection, mitigation, and prevention of attacks against their networks. In effort to assess the potential effectiveness of honeypots in preventing the development and progression of cyber-dependent crimes, we searched in six major academic search engines for studies published between the years 2000-2016 using experimental or quasi-experimental research designs. We could not find any empirical research that investigates the effectiveness of honeypots in preventing the development and progression of hacking incidents, malware infections, and DDoS attacks.