Are Computer Focused Crimes Impacted By System Configurations?: An Empirical Study

Bertrand Sobesto, Michel Cukier and David Maimon

Abstract: This paper describes an empirical study to assess whether computer focused crimes are impacted by system configurations. The study relies on data collected during 30 days on a farm of target computers of various configurations (disk space, memory size, and bandwidth). In addition, some target computers included a warning sign. Following a brute force attack on SSH, attackers randomly access one of these computer configurations and are allowed to use it for 30 days. We monitor network traffic and attackers’ keystrokes to analyze the attack. This paper focuses specifically on the crime, i.e., the use of the computer to launch an attack towards an external target. We define various computer focused crime characteristics (i.e., whether the attack was destructive or not, whether the target was an opportunity or a choice, whether the attack was coordinated or not) and analyze whether the committed crime is significantly impacted by the system configuration.