Jordan University of Science and Technology

Investigating the Detection Capabilities of Antiviruses under Concurrent Attacks

Authors: Mohammed I. Al-Saleh, Fatima M. AbuHjeela and Ziad A. Al-Sharif

Abstract: Cyber security is a major concern of computing systems. Different security controls are developed to mitigate or prevent cyber attacks. Such controls include cryptography, firewalls, intrusion detection systems, access controls, and strong authentication. These controls mainly protect the secure-system properties: confidentiality, integrity, and availability. The Antivirus software (AV) is considered the last line of defense against variety of security threats. The AV maintains a database of virus signatures against which it checks data. Had a match occurred, the AV would have reacted to the threat. Given the importance of the AV, different attacking techniques have been developed to evade the AV detection and render it useless. In this paper, we want to check how the AV behaves under pressure. We make the AV extremely busy in order to bypass its detection. We test several commercial AVs against three scenarios: when data flow from the hard drive (HD) into the main memory (reading), when data flow from the main memory into the HD (writing), and when data flow through the network (sending and receiving). This paper shows that when the AV is overloaded, some malwares can evade detection (in the reading scenario) and enjoy the existence for much more time on the HD (in the writing scenario). Finally, we show that the AVs (or at least the ones we tested in this paper) do not check network data as long as they are not written to or read from the HD.