2019

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

David Maimon

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

David Maimon
Center for Evidence Based Cybersecurity
Georgia State University

Antivirus software is a program designed to keep computer devices clean from malicious software (malware) such as viruses, worms, and trojans, and is commonly deployed on computer and smartphone users' devices as the last line of defense against cyber-dependent crimes). In effort to assess the potential effectiveness of Antivirus products 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.

Our findings reveal that several key approaches are employed by scholars when evaluating antivirus software's performance. The typical evaluations conducted by commercial and scholarly labs are based on scans of collected or synthesized malware samples. While this approach may test the program's accuracy, it fails to consider computer users' behaviors with their computers. An alternative approach for evaluating antivirus software performance is through the use of an on-demand detection tools that can detect both the presence of threats on the scanned computer and the availability of antivirus software. Although informative, these studies are subject to sample selection bias because the samples they employ include computer users who bought the scanning service only. Another approach for assessing the effectiveness of antivirus software employs computer users' self-reports on security incidents they experienced with their computers, as well as reports on the presence of antivirus software on their computers. Unfortunately, these studies draw on survey methodology and may include multiple inaccuracies.

Our research team has identified only two studies employed clinical trials to assess the effectiveness of antivirus products in detecting and preventing malware infections among computer users. The first study by *Lévesque and colleagues'(2013)* was launched in order to "1. Develop an effective methodology to evaluate anti-virus products in real-world environment; 2. Determine how malware infects computer systems and identify source of malware infections; [and] 3. Determine how phenomena such as the configuration of the system, the environment in which the system is used, and user behavior affect the probability of infection of a system" (p. 100). To achieve their research goals, the authors recruited 50 participants from the University of Montréal campus, provided them with new laptops, and monitored these participants' real-world computer usage using various diagnostic tools over a period of four months. The scholars also conducted monthly interviews with the participants and administered questionnaires among them. The authors reported that during the four months of the experimental period, 38% of the study participant were exposed to malware. Accordingly, the authors suggest that almost 1 out of 2 newly installed laptops would have been infected with malware within 4 months if the computers had no antivirus software installed. In addition to determining the overall exposure to malware infection, the authors also explored the proportion of malware infections that went undetected by the antivirus software during the experimental period. They reported that 20% of the study computers were infected by some

form of malicious software that was not detected by the antivirus software that was installed on the machine.

The second study by Lévesque and colleagues (2016) reported a large-scale cohort study that was aimed to test the effectiveness of different antivirus products in detecting and preventing malware infections. Using data collected from millions of computers that had the *Microsoft Malicious Software Removal Tool* and the *Microsoft Windows Defender* installed, these scholars reported results from a natural experiment: malware infection was the outcome, and being protected by a third-party antivirus product was the exposure measure. The authors found that 1.22% of the computer systems in the experimental group were infected by malware during the experimental period. In contrast, 14.95% of the computer systems in the control group could have been infected by malware if no antivirus product were protecting the system. A comparison of the effectiveness of the 10 most prevalent antivirus products (more than 90% of the systems were protected by third-party software) revealed that the effectiveness of these products in detecting malicious software ranged from 90% to 98%.

References

Levesque, F., Nsiempba, J., Fernandez, J. M., Chiasson, S., & Somayaji, A. (2013). A clinical study of risk factors related to malware infections. In *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security* (pp. 97-108). ACM.

Lévesque, F. L., Fernandez, J. M., & Batchelder, D., & Young, G. (2016). Are they real? Real-life Comparative tests of antivirus products. In *Virus Bulletin Conference* (pp. 1-11).