Testing Antivirus in Linux: An Investigation on the Effectiveness of Solutions Available for Desktop Computers

Giuseppe Raffa

Technical Report

RHUL–ISG–2021–3

10 March 2021

Information Security Group
Royal Holloway University of London
Egham, Surrey, TW20 0EX
United Kingdom

Abstract

Anti-virus (AV) programs are widely recognized as one of the most important defensive tools available for desktop computers. Regardless of this, several Linux users consider AVs unnecessary, arguing that the Linux operating system (OS) is "malware-free". While it is true that Windows platforms are considerably more affected by malicious software than Linux platforms, there are several documented cases of malware infections specific to Linux. Moreover, even though the estimated market share of Linux desktop systems is currently only at 2%, it cannot be ruled out that this percentage will increase in the near future. Recent statistics, in fact, suggest that the number of Windows users is gradually decreasing. Considering this and the fact that there is very little up-to-date information about the performances of Linux-compatible AV solutions, the main objective of this MSc project is to evaluate the effectiveness of some relevant Linux anti-virus products.

To this end, we have identified four Linux AV programs, and we have tested them on an Ubuntu Linux distribution against a repository of 43,553 malicious ELF files by running multiple scans over three weeks. This approach has allowed us to evaluate the AV detection rate, to assess the effectiveness of the signature database update mechanism, and to analyse potential regression effects. We have found that the average detection rate of the tested products ranged from 81.8% to 97.9% and that none of them was affected by regression. Unexpectedly, though, only one of the locally-installed AV programs showed a steady increase in the number of detected malware samples, which never exceeded 10 files.

We have also used the on-line malware scanning service VirusTotal to test and compare the performances of 62 anti-virus engines. This was achieved by using a dataset of 4,000 malicious files, which were submitted twice over two weeks via a Python script. While the average detection rate of the on-line AVs was only 59.9%, it is noteworthy that nearly 50% of the anti-virus engines featured a detection rate above 90%, whilst the latter was less than 30% for approximately one third of the AV solutions. It should also be observed that 13 out of 62 anti-virus engines showed regression effects. Furthermore, the results obtained with the locally-installed AV products were compared with those provided by VirusTotal. Only minor discrepancies were found, as the maximum difference in terms of average detection rate was 1.9%.

Finally, we have configured a Kali Linux virtual machine that included the Metasploit penetration testing framework, and we have used six Metasploit payloads to create 24 evasive variants of malware. Differently from the previous tests, these malicious files were scanned and then executed to determine the effectiveness of the Linux AVs' heuristic detection mechanisms. As regards the scan results, the detection rate ranged from 8.3% to 41.7% and eight malware samples were not detected by any AV. Contrary to expectations, the execution of the malicious files highlighted that no anti-virus program was able to block samples that had not already been flagged during the initial scan.

The generated evasive variants were submitted to VirusTotal as well. The results show that the average detection rate was only 16.9% and that 32 out of 62 AV engines did not report as malicious any of the submitted files. In addition, the per-file analysis highlighted that no sample created with Metasploit was detected by more than 26 anti-virus products, with the average being approximately 11.