

Measuring the Effectiveness of Anti-Virus-software

IT Security / Betreuer: Prof. Dr. Endre Bangerter
Expert: Dr. Morton Swimmer, Trend Micro

In the arms race between malware-writers and Anti-Virus(AV)-vendors, the AV-vendors are always forced to develop new techniques to detect yet unknown malware. Testing the efficiency of these new techniques is very complex and resource intensive. As a result, no representative public test results had been available until very recently. Therefore, we have decided to perform our own measurements. In addition, we wanted to provide a service that is able to use the full functionality of AV-software, to scan and detect suspicious files uploaded by a user.



Peter Linder

Introduction

The goal of this thesis was to find out how effective the new techniques of AV-software to detect unknown malware on the end host are. In contrast to the older techniques, the new techniques can only be studied, if the malware is executed on the end host. As manual-testing procedures takes a lot of expensive labour and automated testing very complex, no large-scale tests have been performed since the introduction of the first techniques three years ago. Therefore, current AV-tests leave important functionality of AV-software untested.

Solution

We have designed and implemented an automated large-scale analysis system (AMAS) that has been used to measure the effectiveness of AV-software to detect yet unknown malware, by analysing thousands of samples in a real world scenario. To emulate a user, we have developed a program that is able to detect and interpret alert message GUIs of AV-software. By using image pattern recognition techniques to parse AV-software alert messages, we apply a common interface for all AV-software GUIs. To produce measurements of high quality, we have performed multiple long-term tests and continuously improved the stability and reliability of our AMAS.

Based on our large-scale analysis system, we have designed and implemented an autonomous live service, which can be used to analyse suspicious files by multiple AV-software. Our live service is the first that provides the full functionality of Anti-Virus-software.

Results

We have analysed over 14,000 unique malware samples in 17 days using five different Anti-Virus-software. Based on the measurements of our large-scale test, we could determine that the new scanners insufficiently protect computers with out-dated signature databases. Although Anti-Virus-software experts had expected our results, we can now verify this suspicion for the first time.

To our knowledge, we currently have the only AMAS that can efficiently measure the performance of the full functionality of AV-software.

Additionally, we have developed a live service to where suspicious files can be uploaded for analysis. It is the only known service that provides results collected during the analysis of on-execution scanners. We do provide the full functionality of the tested AV-software.