Memo one of the most common although

Technology, Information Technology

September 11, Memo One of the most common although old fashioned virus detection method is heuristic detection. This method involves detecting and protecting the computer from viruses which were previously unknown hence are not in the virus definition files. This technology is also used to detect new variants of already existing viruses. To do this, the antivirus runs the suspected software on a virtual machine hence monitoring the performance of the software in a controlled environment. If the software being observed performs any malware related activities, the user is notified and the software is prevented from executing on the actual operating system. This is known as sand box testing or file emulation (Malik).

Another technique of doing a heuristic test is decompiling the suspected software's source code and comparing it to known malware source code. If it marches the known malware source code, the user is also notified. This is known as file analysis. Keeping track of known viruses should also be done and investigations done to detect any possible new variants of the same (tools). This is referred to as generic detection.

The basic detection functionality of heuristic detection involves finding false positives and false negatives. A threat to heuristic detection is the constant change of viruses which then may easily infiltrate into the computer system. To curb this, the number of false positives need to be limited and this leads to identification and quarantine of files which are not threats. Heuristic detection can also be bypassed through code injection. Code injection is when the virus software code is split into two parts. The core code which performs the malicious activities and the interface code which provides a mechanism for injecting the core code into the memory and executing it.

Heuristic antiviruses cannot detect this. Metasploit framework is also used to bypass heuristic antiviruses. A stronger form of virus protection software is the use of antiviruses that implement a real time port monitor. This monitor actively identifies any malware that may have bypassed the antivirus (Malik).

References

Malik, Amit. Bypassing Anti-virus using Code Injection Technique. May 2014. .

tools, PC. Heuristic Virus Definition. May 2014. .