Malware bites

August 15 2013

Antivirus software running on your computer has one big weak point - if a new virus is released before the antivirus provider knows about it or before the next scheduled antivirus software update, your system can be infected. Such zero-day infections are common.

However, a key recent development in antivirus software is to incorporate built-in defences against viruses and other computer malware for which they have no prior knowledge. These defences usually respond to unusual activity that resembles the way viruses behave once they have infected a system. This so-called heuristic approach combined with regularly updated antivirus software will usually protect you against known viruses and even zero-day viruses. However, in reality, there are inevitably some attacks that continue to slip through the safety net.

Writing in a forthcoming issue of the *International Journal of Electronic Security and Digital Forensics*, researchers at the Australian National University, in Acton, ACT, and the Northern Melbourne Institute of TAFE jointly with Victorian Institute of Technology, in Melbourne Victoria, have devised an approach to virus detection that acts as a third layer on top of scanning for known viruses and heuristic scanning.

The new approach employs a data mining algorithm to identify malicious code on a system and the anomaly of behaviour patterns detected is predominantly based on the rate at which various operating system functions are being "called". Their initial tests show an almost 100% detection rate and a false positive rate of just 2.5% for spotting

embedded malicious code that is in "stealth mode" prior to being activated for particular malicious purposes.

"Securing computer systems against new diverse malware is becoming harder since it requires a continuing improvement in the detection engines," the team of Mamoun Alazab (ANU) and Sitalakshmi Venkatraman (NMIT) explain. "What is most important is to expand the knowledgebase for security research through anomaly detection by applying innovative pattern recognition techniques with appropriate machine learning algorithms to detect unknown malicious behaviour."

More information: Alazab M. & Venkatraman S. (2013). Detecting malicious behaviour using supervised learning algorithms of the function calls, *International Journal of Electronic Security and Digital Forensics*, 5 (2) 90. DOI: 10.1504/IJESDF.2013.055047