Malware Analysis: A Different Approach

Malware is defined as any code that intentionally disrupts normal computer operation. The best-known types are the virus, Trojan horse and worm, however there are many more different types. While most are mere annoyances, they potentially have dire financial, legal and even national security implications. The malware problem goes back early, with simple "rabbit" programs appearing as early as the 1960's, becoming an epidemic in the 1980's then turning into something with industries and even militaries interested. Strangely, very little has changed in the field of detection since the first antivirus programs came into existence, with nearly all relying on signatures of each individual malware. Given the millions of malware in existence, this leads to many problems, including software bloat and even greater vulnerability to security threats. A new approach that observes the behavior of files on the system and monitors the system itself for any unauthorized changes may prove to be a better, more efficient method of detecting malware. The research presentation will include the history of malware from the major firsts to the major threats of today as well as the motives of the creators. In addition, detection methods will be discussed, current methods will be criticized and a new method will be proposed. The presentation will also consist of a demonstration of a different method for detection based on system monitoring and the behavior of programs running on the system. A program will be developed for the demonstration that monitors changes to the state of the system and detects any potentially dangerous changes to files on the system.

Keywords: malware, virus, security, computer, antivirus, worm, stuxnet, firewall, trojan