TECHNOLOGY

Malware Detection with Download Graph Analytics

OVERVIEW

Background
Malware detection on computers, tablets, smartphones, and other devices is a recurring issue in the software security field, as anti-malware vendors and malware developers use ever more complex techniques to identify and hide malware, respectively. Analysis of malicious executables can be difficult due to obfuscation, hiding, and other techniques to hide and remove traces of malware executables and in memory instances. A useful technique that uses data that could not be easily modified by the malware and is not susceptible to current evasion techniques would be valuable at identifying potentially malicious software.
Innovative Technology
Researchers at the University of Maryland and Symantec Corporation have developed a method to detect malware on personal computers and other devices by analysis of the downloaded executable files on a system. By monitoring download activity and forming a graph of downloaded executables, potentially malicious files can be identified through download patterns. Using machine learning techniques to analyze these graphs, it is possible to quickly identify malware with a low false positive rate and quicker than existing methods. This has an advantage over traditional malware detection methods, as the download graph cannot be easily manipulated, as is common with the malicious executables themselves via obfuscation and encryption.

Patent Pending

APPLICATIONS

· Malware detection

ADVANTAGES

· Quicker identification of malicious samples
· High true positive and low false positive rates when tested with real example data

CONTACT INFO

UM Ventures
0134 Lee Building
7809 Regents Drive
College Park, MD 20742
Email: umdtechtransfer@umd.edu
Phone: (301) 405-3947 | Fax: (301) 314-9502

Additional Information

INSTITUTION

University of Maryland, College Park

PATENT STATUS

Pending

LICENSE STATUS

Contact OTC for licensing information

EXTERNAL RESOURCES

IS-2015-122