Tracking Malicious Executables Using Unsupervised Online Learning

Technology #m05-075

“Lead Inventors: Salvatore J. Stolfo, Ph.D.; Angelos D. Keromytis; Stylianos Sidiroglou

Algorithm to detect viruses in email attachments removes vulnerability to zero-day malicious executables: Existing software technologies for detecting malicious email attachments containing computer viruses or worms rely largely upon existing databases of viral signatures to determine the presence of malicious content. This approach leaves users vulnerable to zero-day malicious executables (i.e. those whose signatures are not yet known) until they are identified and their signatures manually added to anti-virus databases.

Email viruses prevented by learning algorithms that detect malicious executables in email attachments: This technology is an architecture that employs unsupervised online learning algorithms to detect known and unknown malicious executable email attachments. The latter are first analyzed by a filter that can detect the signatures of known malicious executables. Files that pass this test are then executed in a safe virtual environment that emulates a computer running a normal operating system; if the executed files exhibit malicious behavior, they are discarded and their signatures are used to update the filter so that future instances of the file can be immediately identified by the architecture’s filter.

Applications:
• Can protect email users from malicious executables sent by email in large-scale enterprise environments.

Advantages:
• Can automatically learn about and protect users from previously unknown malicious executables without human intervention.
• Advantageous over traditional virus detectors that rely purely on existing viral signatures requiring manual updates


Licensing Status: Available for Sponsored Research Support

Publications: None”

Inventors

Angelos D. Keromytis