Why Evolving Malware Now Requires a Layered Security Approach

A recent spam campaign alleging to be from the IRS is playing on people's fear of the tax man to propagate malware. You may already be familiar with the email with a subject line that reads, "Notice of Underreported Income." It requires the victim to either install the Trojan attachment or click on a Web link to view their "tax statement." This link transports the victim to a malicious Web site where it installs a Trojan that steals information that has already drained millions of dollars from small business bank accounts.

This campaign continues to grow with reported estimates that it constitutes almost 10% of all spam. Testing of this malware has found that only five of the 41 antivirus detection systems used by an anti-virus solution managed to spot it.

An even more recent spam threat disguises itself as a Facebook notification with the subject heading of "New login system". It claims to offer enhanced Facebook account security and attempts to persuade victims to divulge their personal account information. **Anti-Executable stops this type of malicious code from executing and infecting targeted computers.**

Become educated on the threats of malware Just a reminder anti-virus alone is not enough. Malware has evolved and now requires a comprehensive layered security approach that includes both anti-virus and application whitelisting. Anti-Executable doesn't care what new malware looks like, if it matches a known signature, or how it behaves. If it is not on the whitelist – it simply won't run.