Emerging Threats: The Changing Face of Email

By Ryan Naraine
Security Evangelist
Kaspersky Lab Americas

More than three years after the infamous declaration from Microsoft's Bill Gates that "spam will be solved" in 2009, unsolicited junk mail continues to bombard email servers, dumping malicious attachments, phishing lures and spam advertising for fake pharmaceuticals.

According to data culled from Microsoft's malicious software removal tool, a free utility that's updated and shipped once a month on Patch Tuesday, more than 97 percent of email messages sent over the Internet over the last year can be considered spam, with the majority linked to financially motivated malware attacks.

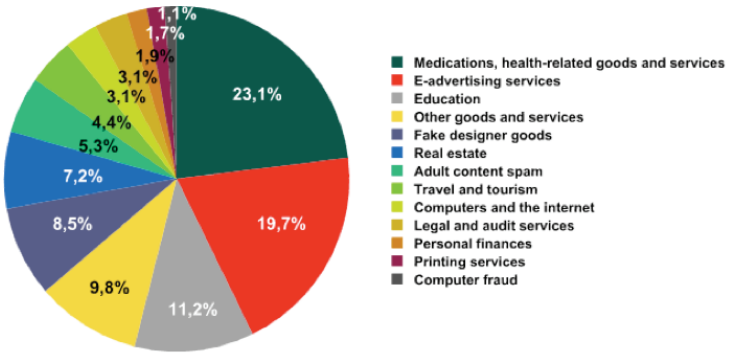
In the past, hackers using email as the primary attack vector relied primarily on convincing end users to click on malicious attachments. The Melissa and Love Letter viruses, for example, exploited the trusted nature of email communications to successfully trick users into executing a dangerous file by using clever subject lines ("I Love You") or promising sexy photographs of tennis player Anna Kournikova. These email attacks, which contained worm-like characteristics, typically harvested email addresses from compromised computers to create databases for future spam runs.

The success of these attacks forced email providers to block malicious attachments at the gateway level and, eventually, end users learned to avoid clicking on attachments. What followed was a classic cat-and-mouse game between attackers and defenders with hackers turning to legitimate file formats (PDF, JPG, MP3, etc.) to serve as the conduit for viruses, Trojans, rootkits and spyware.

Drive-by Downloads

Over the last year, the threat has taken a more dangerous turn with attackers mass-mailing messages with links to infected web sites. These messages contained subject lines linked to sensational news headlines or topical information to maximize the chance of a target clicking on a link.

Spam advertising seen in July 2009



Source: Kaspersky Lab

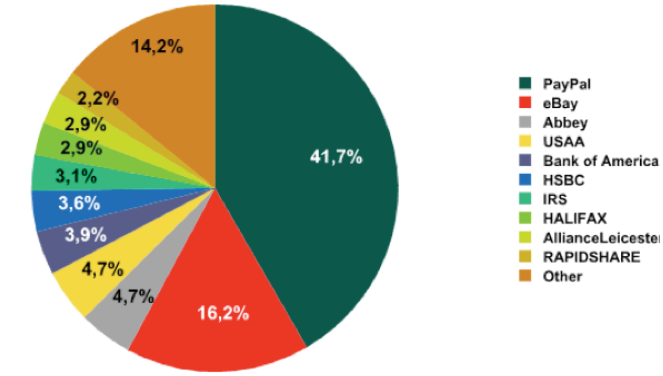
This led to a dramatic surge in drive-by downloads, where malware sneaked onto a computer when the user simply surfed to a maliciously rigged web site. This type of attack simply exploited the trusted nature of e-mails and used social engineering to launch exploits against unpatched desktop applications.

Phishing

In addition to malware attacks and drive-by download lures, email networks are the preferred delivery mechanism for financially motivated phishing attacks. Online banks and other e-commerce/financial services like PayPal and eBay have seen their brands targeted by identity thieves looking to steal usernames and passwords via phishing schemes.

Phishing emails appear to come from online banks or financial services and usually contain a message requesting that the target enter his/hear credit card number, social security number or banking usernames and passwords. The phishing email usually copies the exact look-and-feel of the financial site and contains a link to a phishing site. If a user enters his/her credentials into the fake site, the information is collected by identity thieves and either resold or used for malicious purposes.

Organizations targeted by email phishing attacks in July 2009



Source: Kaspersky Lab

Spear Phishing and Whaling

Another aspect of email phishing is the targeted attacks - called spear phishing. In this type of attack, identity thieves send emails to employees within a specific company or organization. These targeted emails are usually spoofed to appear genuine and may look like it comes from the employee's boss or from a colleague in the HR or IT department. Spear phishing attacks are very difficult to spot and the success rate is known to be high.

A separate tactic, called whaling, involves targeted attacks on senior executives and other high-ranking people within a company or organization.

Botnets

At the center of these email spam operations is the botnet – hijacked computers around the world that are used to launch spam runs on behalf of criminals. Recently, a Trojan attack known as Storm Worm built what experts argue could be the world's most powerful supercomputer. The Trojan, which used a myriad of social engineering lures to trick Windows users into downloading additional malware, successfully compromised between one million and 10 million CPUs, producing computing power to rival the world's top 10 supercomputers, according to New Zealand computer scientist Peter Gutman.

Recommendations

Email networks are a crucial spoke in the malware distribution wheel and, as the volume of spam rises, consumers and businesses must take extra precautions to keep up with the sophisticated nature of attacks.

1. Invest in robust anti-spam and content filtering protection. This allows you to stay ahead of blended threats that combine unsolicited email with web-borne attacks.
2. Combine anti-spam technologies with anti-malware solutions to intercept and block executables and other malicious content from infecting systems.
3. Keep all third party desktop software, browsers and operating system patches up to date. This reduces your exposure to drive-by attacks.
4. Make sure employees are educated about the risks presented by email-borne attacks. This education should include safe browsing habits.