



The Security Minute

Take a second to be secure.

A communication of the Longwood University Information Security Office

New Malware Threats Take Computers By Storm

In 2007 malware creators demonstrated their devious capabilities through the introduction of malware that was more malicious than ever. Computers became infected with this year's most prolific malware, the Storm worm, when users clicked infected links or opened infected attachments in spam messages. The infected computers then became members of the Storm worm's massive botnet, an army of remotely controlled computers used to send spam and launch attacks on other computers. Large amounts of spam, such as the loads sent by the Storm worm botnet, have the potential to overload an e-mail gateway and similarly the botnet may also send so many requests to a network or website that the resource is rendered unavailable (in what is known as a denial of service attack). Fortunately the spread of the Storm worm and other similar malware can be slowed through understanding this evolving threat and the simple steps necessary to protect your computer.

Key Characteristics of Evolving Malware Threats:

1. Organized attack

Computer viruses of the 1990s were often pranks or experiments; however, increasingly malware is being associated with organized crime and the market for malware is a part of a flourishing underground economy. Computer viruses created annoyance and disrupted business; however, botnets can also create value and can be sold or leased for profit. The Storm worm botnet's creators launched attacks against universities, security researchers and other malware creators (in an attempt to eliminate the competition) and sent numerous rounds of spam messages, including introducing spam messages that carry PDF and MP3 attachments.

2. Diverse tactics

In order to avoid detection and infect as many computers as possible, the Storm worm botnet changed tactics frequently. The subject lines and contents of spam messages were changed in hopes of evading spam filters and to catch individuals unaware of the creators' latest tactics and while some Storm worm messages used infected links others used infected attachments to prompt the installation of the malicious program. In addition to changing the messages carrying the malware on a frequent basis, the actual malware changed in an attempt to avoid detection by antivirus software and infect as many computers as possible. Due to the size and strength of the botnet the creators were also able to experiment with other tactics such as spamming blogs with infected links to recruit more unsuspecting botnet members.

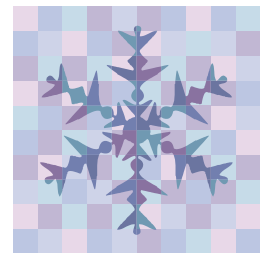
3. Sophisticated social engineering

The Storm worm's most memorable tactic was a run of e-greeting card spam during the summer that tricked users into opening the messages that were supposedly from a "friend," "neighbor" or other nameless relative or acquaintance. Later Storm worm messages showed an understanding of American pop culture, promising a program called "digital puppies," videos of Beyonce and an NFL game tracking program offered on NFL opening weekend. Legitimate looking e-mails offering services of interest to individuals were able to gain more members to the botnet and ensure a ready supply of computers for attacking or spamming for most of 2007.

How do you protect yourself from the Storm worm and similar malware?

1. Delete all spam messages and avoid following links or opening attachments in any message you suspect may be spam.
2. Run up-to-date antivirus software.
3. Keep your operating system updated with current security patches.

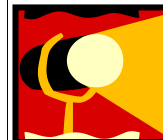
December 2007



What is ... malware?

According to Microsoft, "Malware' is short for malicious software and is typically used as a catch-all term to refer to any software designed to cause damage to a single computer, server or computer network."

Viruses, worms, trojans, rootkits, bots, spyware, keystroke loggers and phishing software are all various forms of malware.



Security Spotlight

Virginia Information Technologies Agency (VITA) offers monthly tips for protecting yourself online. This month's tips focus on avoiding phishing attempts.



The Security Minute will be a monthly publication designed to raise awareness of information security related issues and concerns. Look for upcoming issues of The Security Minute and other security awareness initiatives.