Spam development - Part 1: New tricks

While you're sleeping well, your computer may be working as a peer-to-peer spam or node server, providing a source of processing for a malware network that pulls in any form of criminal activity. online.

While you're sleeping well, your computer may be working as a peer-to-peer spam or node server, providing a source of processing for a malware network that pulls in any form of criminal activity. online.

Spam is used by botnet exploiters in a variety of new forms (such as hiding behind the release of Storm - a spam-malware hybrid) to build distributed robot networks (or botnets), causing the spam recipient's computer to become 'zombie' in the network. These zombies come together as an 'army' and they have a great competitive ability that sometimes surpasses the strongest supercomputers.

The problem is more difficult to solve when legitimate transactions, adjustment and execution modes are combined.

Change faster

Storm is a combination of spam and malware and it is estimated that they have spread to about 10 million computers, this number will continue to increase in the near future. However, there is currently no way to know how many computers are infected at the same time.

The rapid development of the spread rate suggests that the complexity and scale of current botnet dispersers is changing.

Spam is becoming more sophisticated. In the past 12 months alone, it has seen sudden changes, they have grown by a decade ago. So most importantly, detection methods need to grow fast to keep up with new spam technologies later on.

Detecting spam and preventing it scientifically must be promoted faster and maintained longer.

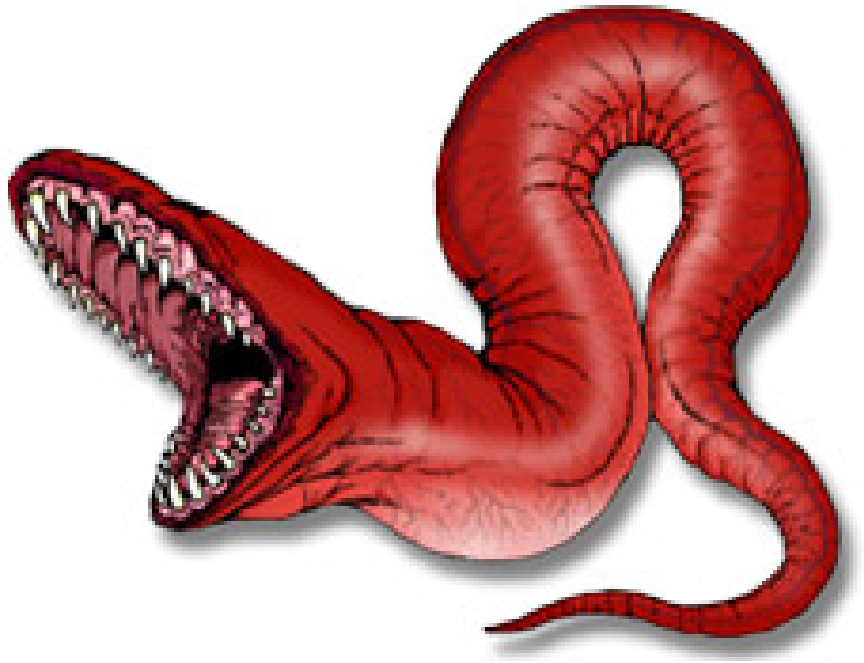
Anti-spam programs must be implemented with a variety of solutions while simultaneously maintaining the level of protection as well as tools. This means increasing processing time through a variety of tools, increasing the cost of product or service products by firms and expanding the potential for increasing the defect rate.

Storm's rise

After a quiet period, spam attacks followed the trend of Storm massively once again warning security researchers. Spam links to MP3 audio files, YouTube videos and Adobe pdf documents are used to trick recipients into downloading infected attachments or when users visit websites that contain malware. More dangerous is the spread through computers and bringing them into a remote controlled network.

This latest development wave is based on an attack on spam following the trend that Storm has taken before. It leads the recipient to fall into a phishing business system to gather information from the user.

According to Kaspersky, this is the first series of email spam using special graphics files that contain background audio (such as Adobe's .pdf files) to bypass spam filtering systems.



The creators of Storm and spam are even more dangerous when they "eat" the events or topics at the right time (like dancing with skeletons on Halloween, cheap drugs, announcing offers to link to Popular videos on YouTube, greeting cards and service ads .) are intended to attract recipients to open attachments or links to unsafe web sites.

In general, Storm spammers also constantly change the way to avoid spam and security defenses on other

computers or networks.

Researchers at Kaspersky also made an assessment in a recent virus list announcement that ' *Spammers once again create several types of attacks to renew the technology used when creating attachments. graphics in email spam (photo spam) during the first 6 months of 2007* '

Image spam is a huge problem for two main reasons:

The first is that simple identification of a photo is not always effective. Just changing a few pixels of pixels will break the traditional identity. There are millions of changes that can be applied without affecting the image content.

The second is that spammers use links to images that are placed on multiple websites. The image itself is not in the email until it is opened. Photos can be stored on websites of large companies that have been controlled by them and botnets use millions of legitimate email addresses to deliver mail.

Resilience to recovery

Although it is not often publicized as to embed code to remove the hard drive, disable the computer or install a keylogger to catch confidential data such as passwords, the Storm or Trojan worm has also proved that they are the most adaptable malware.

Spam Storm has demonstrated adaptability and extremely quick code changes based on spam filters or other defenses they encounter while trying to bypass network or computer protection.

Storm uses complex programming techniques to automatically repack herself. This is similar to someone changing costumes every 5 minutes during a small party. The inner nature is the same but the appearance has been changed. The creators of Storm kept track of how they were discovered and then launched new

countermeasures.

It was the programmers Storm's diligence in avoiding detection that created a high-end malware.

This is just a simple way in many ways botnet uses to send spam. Basically, Storm does not spam better than other botnets. But it's better at self-installing and launching to avoid detection.