The Future of Bot Worms

What we can expect from worm authors in the coming months

by **David Sancho, Senior AV Research Engineer**
Trend Micro

The current trend in worms seems to go the bot route. Bots—programs that operate as an agent for a user or another program—are most often seen as malware and keep attacking unsuspected users in surprisingly high numbers. This document details the possible new additions and modifications that bot authors might incorporate to their hideous creations in the very near future.

Nowadays all bots worms are built in a modular fashion. This means that the creator of the program can choose among a number of different attack methods, including vulnerability exploitation, mass-mailing, P2P (peer-to-peer) propagation as well as the parameters for each of them. The result is a worm *ad hoc*, specially engineered to accomplish its objectives: stealing information and keeping control of the infected computer.

The idea of modularity in these types of worms has been confirmed in WORM_RBOT.CBQ and WORM_ZOTOB, two network worms that grabbed headlines globally this week. Network vulnerabilities can be used as a propagation method as soon as the exploit is available. When a piece of code is written to exploit a certain vulnerability in an operating system and is published on the Internet, the creators of these worms can just attach it to the old code of the worm, recompile it and voilà—a new dangerous worm is ready to be unleashed.

Thus, this means shorter times to achieve network exploitation in the very near future. Below is a list of network vulnerability exploitation times for some prominent worms:

WORM_NIMDA:	366 days
WORM_SLAMMER:	185 days
WORM_BLASTER:	26 days
WORM_SASSER:	18 days
WORM_ZOTOB:	4 days

The end result: Because worms nowadays can be created at such rapid speeds, PC users worldwide face even greater threats. The possible ways we can fight against this are:

1. Patching home systems immediately as the updates are made available on the Microsoft Web site. Automatic updates are just not an option anymore. The security of our home systems is at stake just by being connected to the Internet.

2. In corporate settings, deploying software and hardware systems that specifically defend against these threats. Detecting and blocking the network packets that the worm uses to exploit the vulnerability is by large the best prevention to not get hit by this kind of malware. These systems include IDS (intrusion detection systems), specific network-antivirus systems like Trend Micro Network VirusWall® or Trend Micro Personal Firewall,

which can block the reception of shellcode packets even if the underlying system is still vulnerable.

Other technologies we can expect future worms to include:

RSS Feed hijacking: As the name implies, this evolving technology is a method to get "Real Simple Syndication." Web pages can update their contents, and their RSS subscribers will get them as soon as they are published by means of an RSS-feed client, which frequently looks for new content. The easy way of taking advantage of the popularity of this rising technology is to hijack the existing configured feed clients to automatically download new copies of worms and other threats to the infected computers. This is accomplished by pointing the already-configured client to different and malicious Web content. The way this would work is checking if the system has any automatic feed download configured. If it does, it would just add or change an existing one to point to the malicious Web site. This kind of attack would have two direct outcomes:

1. It would serve as a passive download point, starting connections from a legitimate point. Since the source of the connection is already "allowed," it would bypass personal firewalls and other barriers.

2. The download would still be working even if the worm is detected/deleted. To get rid of this properly, there should be a cleaning tool that deletes the configuration in the feed client.

As a mitigating factor, there is no standard in the current use of these programs, so the attack would have to choose specific software. This form of attack is not highly dangerous right now.

However, all this may change when the new Internet Explorer 7 is finally released. Microsoft is already announcing that the new version of the popular browser will have built-in support for RSS feeds. This will open some interesting possibilities to worm creators.

To fight this, companies should deploy, if they haven't already, a method to scan HTTP traffic, as this will likely be a very popular method of spreading near-future malware.

A new possible future technique that we have to be aware of is:

Polymorphic shellcode exploit attacks. Some researchers believe that the authors of these bots might be able to create a module that changes the exploit code so that it varies every time, but it always has the same result. Since most IDS and vulnerability detection relies on malware using the exact same exploit over and over, if the fingerprint of the exploit code changed every single time, it would be able to bypass the scanners and have far-reaching effects. Though this is theoretically possible, in the event that such a module was created, the attackers would need to be able to understand how the exploit code works and how it can be modified. These concepts are in conflict with the aforementioned trend of incorporating a new exploit as soon as possible and would slow down the creation of the worm. They would probably have to choose between a fast attack or a stealth attack. Hopefully, this will remain theoretical, but it's a dangerous possibility to consider.

To combat against these bots, antivirus companies have long realized that the only difference among many variants of the same worm is the different **compression methods** used. Worm authors compile the worm and compress the newly created executable in a different compressed .EXE file. When antivirus vendors detect it, the authors just recompress it with a different algorithm and start the process again. There are hundreds of different compression algorithms to use, which makes the detection of bot worms not an easy task.

The tendency is, of course, to be able to detect different compression methods before isolating specific detection patterns. Expect new advances on this in the coming months. Trend Micro is already working in a scan engine that can detect compressed samples. Trend Micro scan engine 7.7 is expected to be released early next year, and it is designed to detect bot worms as soon as they are being released—thanks to this new detection technology.

Bot worms are the most dangerous pieces of malware currently in the wild. Users need to be aware of them and the methods they use to infect other computers in order to prevent being affected by them. This document tries to point out possible future attack avenues to raise awareness about new technologies and their possible misuse.

About Trend Micro

Trend Micro Inc. provides centrally controlled server-based virus protection and content filtering products and services. By protecting information that flows through Internet gateways, email servers, and file servers, Trend Micro allows companies worldwide to stop viruses and other malicious codes at a central access point before they reach the desktop.