appeared on 3rd Mar 2010

Spy vs Spy in the Internet

Malicious software agents find ways to duck measures to stall them, says S.Ananthanarayanan.

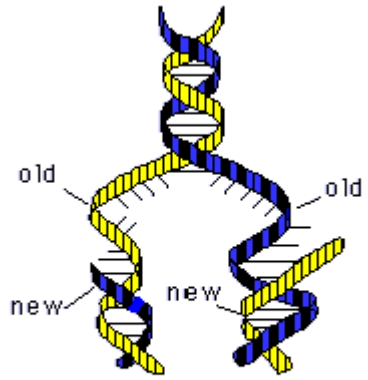
The simple days of viruses that attacked individual computers have changed since the advent of distributed computing. With the growth of the Internet and the power of personal computers, there is much sharing of computing power of computers, to manage tasks that need massive computing power. This technology is also serving the ends of malicious software, that recruits vast numbers of compromised computers to carry on its nefarious business.

The viruses

The word, ***virus***, in computers, comes from the same word in biology. The biological virus, in fact, is little more than the information of a cell that helps reproduce itself – ***a strand of DNA***. The DNA is a complex molecule chain that contains the genetic code of the cell – particularly what proteins the cell will produce, or what action the cell will take when it comes into contact with enzymes or other means of signaling between cells.

When a cell is ready to reproduce, the DNA molecule, which has the shape of an 'interlocking' double helix, separates into its two 'complementary' strands. From the surrounding chemical 'soup', each strand soon collects the exact match at every bit of its length and the strands become 'copies' of the original chromosome.

The cell then splits into two, each with a copy of the coding to produce various kinds of proteins, enzymes, etc, which defines the identity of the cell.



Each strand grows a new partner

The virus is a cell which has not the complexity of a normal cell, to generate proteins, respond to signals and the like, but just the bare information necessary to reproduce. When the virus infects a cell, then, it begins to do the one thing that it is capable of, which is to reproduce, and begins to consume all the host cell's resources. The host cell then becomes defunct for its own function – which leads to disease and all else.

When the host cell is full of copies of the virus, it bursts, and the multitude of viruses spread out to infect other cells. The actual infection takes place by the virus having an

exterior that exactly fits a particular kind of cell and this is the reason that that virus are very specific in what they infect, and the disease that follows.

The computer virus

The computer virus is a piece of code that acts in the same way. Its basic function is to create copies of itself. In the process, it could use up the computer's resources and stop or slow down the computer's functions. And this is the reason that Frank Cohen, a PhD student in the early 1980s in California, who first thought of such 'self-replicating' software, suggested the calling the software a ***virus***.

While most viruses were first only of this 'reproducing' kind, the more malicious varieties could take definite action, like preventing booting or corrupting files or even formatting the hard disk. And later versions of viruses would seek the computer user's address book, when the user was on line, and email copies of the virus all addressees, to infect them too.

The industry reacted vigorously and developed software that could protect computers against virus-type activity. With rapid information sharing information of virus attacks, code to seek out characteristic features of the coding of different virus was developed and distributed as 'antivirus software', to identify and neutralize such code when it accessed the computer.

Distributed computing

Although personal computers have now become powerful, much of this power is normally not used, while the computer serves only as a word processor or to support some stand-alone programme. But there are applications, like sorting, searching, data mining, that require huge resources to manage with acceptable delays. Rather than provide huge computing power, there is now an option of sharing the spare resources of all computers on the network. With hundreds of computers on large networks, and thousands on the Internet, distributed computing is both an economical and resource conserving alternative.

It is now routine that the specially programmed computers poll all terminals on the network and assign to them portions of the larger task, to be carried out in parallel, where possible, so that the main task is done in the shortest time. The trouble is that this same technology is also available to agents that manage malicious software, to manage the new objects that have now arisen for such software.

Botnets

The well-known virus attacks, like ***Melissa, Love letter or Sassar***, have not recurred since 2004. This is not because antivirus measures have become effective, but more because the objectives of malicious software have evolved. Rather than only cause annoyance or even carry out apparently motivated actions, like ***denial of service*** or

spreading spam, the stress is now in stealthily collecting information from affected computers, including key-stroke data for theft of passwords of bank accounts and credit cards.

Keeping watch on thousands of victim computers is a demanding task and there is flourishing industry of recruiting unwitting computers to join hands. The computers affected are not disabled but only, more usefully, their spare capacity is commandeered. Once affected, the computers work by themselves, as robots, or ***bots***, programmed to do the master's bidding and a network of such computers is called a ***botnet***.

The Botnet administrator or the ***bot herder or bot master***, communicates with the compromised computers through a channel like ***Internet Relay Chat*** or ***Instant Messaging*** programmes and can control the group and direct their activities. While such activity violates the IT laws of all countries, it is estimated that a quarter of the computers connected to the Internet are part of ***botnets***. Policing agencies the world over are detecting and removing botnets, the number of whose nodes runs into millions.

Strategy

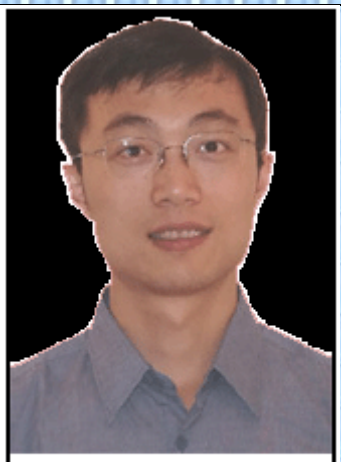
Like real life criminal groups, botnets need to constantly recruit new computer terminals, as existing ones get discovered. It is this overt contact by self propogating botnet software that provides the means to discover and neutralize the menace. Specially equipped computers are installed in the network, with dummy activity that mimics real credit card transaction, etc.

This kind of luring the enemy to make contact and get compromised was used in cold war espionage and counter espionage – to lure spies or high officials, usually into sexual encounters, known as ***honeytraps*** or ***honeypots***. The word, honeypot has passed on to the special computers which are placed in networks to lure botnet attacks.

Honeypots serve two purposes – one, to keep the bots busy with dummy nodes, thus leaving the important victims alone and – second, to provide system administrators with a ring side seat to view botnet activity. As there is no legitimate reason for any computer to make contact with honeypots, all contact is known to be 100% malicious. When an intruder has broken in, her methods and weaknesses can be analysed, to protect other nodes. The network traffic of the botnet can also be identified, to clean other bots and also to locate the botnet master. In this role, the honeypot effectively uses botnet software to compromise the botnet!

The war goes on

A paper in the International Journal of Information and Computer Security, by Cliff C Zhou of the University of Central Arizona reports that like cold war spies, botnets can also be primed to be wary of honeypots. As honeypots, which invite botnet attack, are themselves a security risk, they need to be disarmed so that they do not become a part of the botnet rather than a spy within the botnet. This initial reluctance, when contacted by



Cliff C Zhou, School of Computer Science, Univ of Central Arizona

the botnet, could blow their identity – so that the botnet either disables them or simply ignores them, say Zhou and his associates.

“By revealing this vulnerability to the computer security industry and presenting possible guidelines for creating honeypots that might be undetectable, the team hopes to pioneer a way to trap and block Botnet software before the Botnet controllers are able to exploit this technical loophole in legitimate computer systems employing honeypots”, says a press release.