

FEATURE

THE LIFE CYCLE OF BOTS

Luis Corrons

Panda Security, Spain

I have spent a lot of time thoroughly analysing how bots work – studying the overall bot ‘ecosystem’ as well as the individual files. It is curious to see how they have achieved a certain level of autonomy, in such a way that they almost have a life of their own. We are still a little way from Skynet [1], but it is only a matter of time ...

CONCEPTION

As with all life cycles, the starting point is conception. One of the most effective and effortless methods of creating a multi-functioning bot is to use a framework. We must also bear in mind that bot source code is available on the Internet, so anyone with a basic knowledge of computers can make a bot. Of course, there is always the option of programming your own bot from scratch, but this is rarely done these days.

Once finished, the bot creator usually distributes and sells their ‘creature’ as if it were any other customized software program. We could compare buying a bot with buying a pet, where the customer can buy the pet that best suits their needs. But, of course, there are many more options with bots than with animal breeds. I won’t list them all, but some of the most typical options are the following:

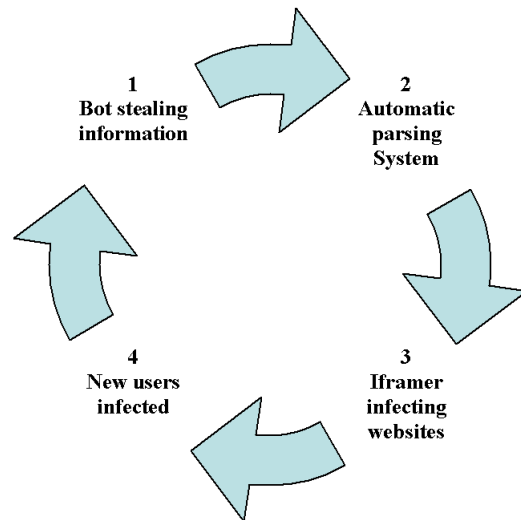
- Sending spam.
- Launching DoS attacks.
- Stealing information (banking information, information from e-shops, email accounts, all type of passwords, etc.).

Of course, the bots are provided with updates and guarantees that when they are sold, no signature-based anti-virus program will be able to detect them.

GROWTH/REPRODUCTION

Now we have the little baby, it’s time for it to grow up and reproduce itself. First, the creature needs to infect at least a small number of computers. There are many ways to do this, though the most common methods involve infecting websites with kits similar to MPack [2], or sending spam.

Having infected a few PCs, the bot creator only needs to sit back and wait for the new ecosystem to develop on its own. This is one of the most fascinating phases in the cycle of malware. Some hackers have managed to create complex systems from which they get feedback. Let’s explain it step by step:



1. The trojans (bots) start working by stealing the user’s data and uploading the logs to the corresponding server.
2. In the server, the logs are parsed in search of ftp accounts, storing the data in a text file.
3. An ‘iframer’ application accesses the file containing the information from the stolen ftp accounts and starts accessing all of them automatically. The application searches for certain directories and modifies the pages hosted there with iframe tags that point to an infecting server (with MPack, WebAttacker [3] or any other similar system). Tools such as IcePack [4] incorporate the functionality of the infecting server, ftp account checker and iframer in the same package.
4. The infection system only has to wait until users visit the (legitimate) websites whose pages have been modified. The user is infected with a trojan that is small (a few kb) and silent (it displays no messages), and whose sole function is to download and install more malware. The malware downloaded may be the trojan downloader itself. We have seen in the installed servers, systems that allow the trojan to change its shape every few seconds or even a different one for each computer, in order to avoid anti-virus signature detection and ensure the longevity of the trojan.
5. The data of all the newly infected users is uploaded to the server (1), where it is processed to extract new ftp accounts (2) in order to access websites and infect them (3), thus starting the cycle again.

DEATH

There are a number of different factors that can lead to the death of bots:

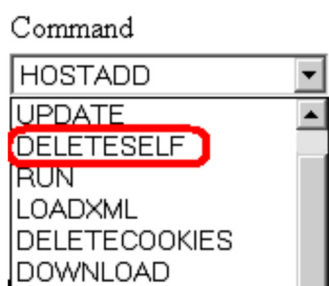
Predators

Firstly, we must mention anti-malware products, especially those which include proactive technologies rather than relying on signatures to detect the bot (detection is thus harder for malware to evade).

Secondly, we must mention other strains of malware. In order to protect themselves from detection by security programs, it has become common over the last several years for certain strains of malware to monitor systems for the existence of certain other malware. If it finds any, it will delete them from the system by ending their processes, deleting their files and registry entries, etc. Later, these strains of malware evolved and we started to see them monitoring systems for the existence of (and removing) other rival worms/trojans, and even older versions of themselves. By doing this the malware can minimize the instability of the system and the resource consumption of the computer, as well as getting rivals out of the way. Only the strongest can survive.

Suicide

A curious option we have seen in many bot control panels is for the hacker to send an instruction of self-deletion to all the bots, which means the end of their existence.



Overpopulation

There is a theory that overpopulation of the planet may lead mankind to his own extinction. But let's not get our hopes up over the same being true for bots: the critical factor in overpopulation is not so much population density as the availability of resources for the population – and for this reason we must rule out this option for bots.

Log poisoning

This is a technique I have seen carried out by some banks when their servers have been under attack. Log poisoning involves the infection of several computers, which start flooding the server with false data. The poisoning is smooth but ineffective. The processing of the log data is quite automated and, therefore, it will only lead to an increase in information storage and processing.

In any case, the problem with each of the previous points is that we are talking about the death of the trojan. Let's look at the situation from the perspective of the whole ecosystem. Although anti-virus programs detect and delete the trojan, the downloaded trojan changes constantly, rather like the mythological hydra [5] – when Heracles cut off its head it grew back two more.

The best way to shut this ecosystem down is to shut down the servers. While this may sound simple, it can be very difficult to carry out. These servers are usually hosted in countries like China or Russia, where taking them down is more than an awkward task, it's almost impossible. The server hosting the infection kit is usually different from the server to which data is sent and there may even be multiple servers.

Furthermore, there's no use in just closing the server to which the trojan sends the data (which is usually the one which hosts the control panel), as the users are still infected and in many cases downloaders are active on their machines. This means that the hacker can easily install a new version of the trojan that sends the data to a new server.

What else can be done? The most effective solution would be to kill (metaphorically speaking) the bot's creator, which brings us to the final point:

Law enforcement

I know that this will bring a smile to many readers' faces (as it does to mine), as the general feeling is that those behind crimeware are light years away from being tracked down by law enforcement agencies. This bears some truth, though the aim of this article is not to go into the situation in depth. Regardless, many people agree that some law enforcement provided with the necessary means, international collaboration agreements and proper legislation could be the best solution. However, we should be mindful of the fact that we will never be able to terminate all bot ecosystems and other malware completely, just as the police will never be able to stamp out all crime.

REFERENCES

- [1] http://en.wikipedia.org/wiki/Skynet_%28fictional%29.
- [2] http://blogs.pandasoftware.com/blogs/pandalabs/archive/2007/05/11/MPack-uncovered_2100_.aspx.
- [3] <http://www.websense.com/securitylabs/blog/blog.php?BlogID=94>.
- [4] http://blogs.pandasoftware.com/blogs/pandalabs/archive/2007/07/26/Ice_2800_Pack_2900_-for-the-summer.aspx.
- [5] http://en.wikipedia.org/wiki/Lernaean_Hydra.