UNIVERSITA' DEGLI STUDI DI ROMA TOR VERGATA

FACOLTA' DI INGEGNERIA

Corso di Laurea in Ingegneria Informatica

Tesi di Laurea di Primo Livello

Analisi Comportamentale di Malware Botnet-Related

Relatore:
Prof. Giuseppe F. Italiano

Candidato:
Lorenzo Paris

Correlatore:
Dott. Giovanni Bottazzi

Anno Accademico
2015/2016

Summary

The continue expansions of the devices connected to the Internet network, is inducing the cyber-criminals "community" to design more and more advanced and efficient techniques for unauthorized accesses into the systems itself; for this reason, the Cyber Security subject becomes a complex and essential topic.

From a report of 2015, it seems that more than 32% of the world population has accidentally and unconsciously installed a Malware inside their devices. Particularly, this thesis is targeted to the study and the analysis concerning to a particular sort of Malware, whose aim is to build an infected network of devices (stand-alone or mobile), the widest possible, remotely monitored by means of one ore more C&C Server (Command and Control). This sort of networks is called Botnet.

Botnet, in fact, is a network of infected devices remotely monitored by the so called Botmaster, used for a wide range of illegal purposes such as DDoS Attacks, Pishing, Spam, Ransom, and so on.

The feature which marks this kind of Malware is their peculiarity to contact the respective (even several) Command & Control Server by an high periodicity.

Nowadays exist a lot of analysis techniques for intercept the cadence of this kind of connections. The most used is the Fast Fourier Transform, which is believed having the flaw to be quite intricate at the computational level. The following thesis, conversely, makes use of a new methodology which allows to minimaze the requirements in terms of memory used and computational complexity.

In order to test the reliability of this method, has been developed a virtual environment makes up of a series of Clients and a Server which will works as gateway for the clients themselves.

First of all, has been simulated the behaviour of a Malware through two simple Java programming codes. In the first test, a client carries out some HTTP requests toward a prearrange domain at regular intervals. In the second test, increasing the

complexity level, the client carries out some HTTP requests toward the default URL, by means of random intervals inside a fixed range.

At the end of the tests, through the data provided by the Server, has been analyzed the behaviour of the client by means of a series of computations belonging to the proposed method. The analysis results actually seems to reveal the exact value of the connections' frequency previously set up at the code level.

Subsequently, has been studied and analyzed, through the method itself, the periodic behaviour of 3 real Malware:

1. **DriveDDoS**: resulted the most active among the three, has as a modus operandi the one to execute DDoS kind attacks;
2. **Andromeda**: having inside an Anti-Virtual-Machines system, it has proved the most sophisticated among those analyzed;
3. **NjRAT**: it is a Remote Administration Tool, namely it provides all of the tools for having the total control of the infected machine.

The frequency with which occurs the connections between infected device and Command and Control Server, is an extremely important factor for the purposes of scalability of the Malware itself. This peculiarity in fact has been confirmed and analyzed for all the Malwares proposed in this Thesis. Particularly, the used method has been shown to be particularly reliable and very simple at the computational level.

Because of the high rate increasing of devices connected to the Internet network, it becomes more and more important the protection measures offered by the Cyber Security experts. This method, still under experimentation, might be part within the wide range of tools used for the analysis of the passive traffic produced by malevolent softwares.