SITAIBA 2021 Keynote Speech

Attack and Defense of *ad hoc* Botnets

Patrick S. Chen (chenps0711@gmail.com)

Abstract

Distributed Denial of Service (DDOS) is one of the greatest threats to information security, and it often causes big loss for businesses. Before the attack, the llegals usually organize a large number of network bots, also known as Botnet, under their control. The number of bots can be several thousands, even several millions; they are organized in a loose way. However, with the development of technology, the connection among bots could be broken or disintegrated, and the survival period of the botnet becomes an interesting research topic in the information community. On the defender side, though information tecnology professionals often adopt security measures or counterattacks to defense DDOS, but this kind of approach is mostly static, unable to effectively protect security of the system because after years of development botnets seem to have enhanced their concealment and increased their survial periods.

It is reasonable to assume that a malicious attacker might think from another perspective, randomly building a network of robots, rather than organizing a pre-connected a large number of computers or devices so that security personnel cannot detect or destry it. The attackers might construct this unlinked network by scanning the communication port to find objects that can be compromised, and then finding some less protected computers or devices as priority targets for their first-wave attack. After this, hackers can begin to expand the construction of peer-to-peer distributed networks of robots. Because the network built in this way is unpreingrammed, the configuration of the botnet is random, and each attack lauched from it is different. For example, fastflux technology is used to avoid detection by constantly changing the system IP. In common days, they are just preparing and deploying an attack. Once an attack to a particular target is determined, the controller will issue a Command-and-Control directive to the botnet to attack jointly.

Knowing each other is the key to beat opponents. In this study we used brute-force password cracking to construct a small robot network virtual environment for experiments to obtain necessary simulation parameters, such as time to control an equipment, attack data flow, dynamics of robot network formation, etc. Then, based on these resulting parameters, we used simulation software ns-3 to simulate the attack on a particular target using different sizes of robot networks. We observed the attack processes, the number of netbots used, the time of a successful attack needed, the data flow generated by each attack. Simulationresults reveals that a bot might generate 2 Mbps data flow, and we could geneate 3.6Tbps data flow within 10 minutes if we could organize a network with 3 million bots, meaning that it could crash any system. Though there are few litertures on DDOS attacks lauched by such *ad hoc* botnet, it is not taken for granted that hackers would not come up with a similar approach.

Starting from the perspetive of attackers, we studied in ths paper how to improve the life length of a botnet based on the existing robot network. It enables us to gain a deep understanding about the evolution of botnets through the attacks implemented by bot masters, the way they protect their bots from being detected, and the process of a DDOS attack.We also observed that bot masters are gaining more power to control over his botnet, in which *ad hoc* network is hard to detect by security monitoring, and the dynamic configuration allows a bot to rejoin the network when it loses contact with its peers. Therefore, this exploratory study provides a valuable reference for academicians and information security professionals.

Keywords：Botnet、Brute-Force Decryption, P2P Network、Fast-fluxTechnique、

Distributed Denial of Service (DDoS)