879 words

Distributer denial of service/Botnet attacks

1. Introduction

Botnets are networks of illegally controlled computers typically employed for malicious activities (Grizzard et al., 2007). They are created by infecting a computer or more with a malware through attachments received in emails, infected USB drives, malicious web sites and many others. Their role is to allow the bot master(attacker) to take control over the victims computers and do a lot of harm at once through malicious activities such as email spamming, DDoS attacks, key logging, hosting of illegal files, identity theft etc. Botnets are able to update themselves so nobody would be able to detect them and they can deactivate Antivirus software's and install more malware programs to make them harder to delete.

2. Analysis

Nowadays, Botnets are the most common channel for cyber-crimes. They can do a lot of harm in a very short time and they won't even get the blame for it, because they're using hosts to carry their malicious activities to the intended victim. As a normal person, attackers aren't interested in your personal data or to harm you in any way possible, unless it's in their interest, but they'll use your computer as part of a Botnet network. Since the growth in number, Botnets have attracted a lot of attention on them. Researchers started gathering information on their behaviour to understand their structure better and what they're capable of.

Detecting a Botnet is harder than it seems because the attacker makes sure of that and it also can't be done by anyone. However, there are methods to detect them: active and passive. The passive methods are the most used ones because they can't be detected right away, but they're not always efficient when it comes to new bots (signature-based methods). The detection process requires more than one passive method as well as active methods.

The Internet of Things poses new threats to our data every day, new attacks occurred and new Botnets got discovered. Last year a very threatening bot, the successor of Mirai DDoS Botnet, was discovered. Satori is a new and not sophisticated Botnet that can be launched by any low-level cyber-criminal and can do a lot of harm with little effort.

In addition, in February 2018, the first documented native IPv6 documented attack has occurred. It originated from around, 1,900 native hosts on more than 650 networks. The attack brought new malicious methods and highlighted that new things are there to come.

There are plenty of ways for an attacker to take over the victims' computer. Spamming is the most common way to do it, as well as hosting of illegal files and phishing. Every day we get spam in our inbox, but we don't know if they're harmful or not and that's why we shouldn't open them, especially if they contain attachments. Hosting of illegal files is a completely different story because you can actually get in serious trouble with the law because of a simple file that you downloaded. The most known incident is the one that includes The Pirate Bay: the website is famous for its on point content, people can download basically everything through it with the use of Torrent, but the content doesn't necessarily belong to them. However, since 2012 they were shut down multiple times for owning illegal files and they even got jail time for it. Another easy way for attackers to do harm is through "Pay-per-click". The attacker may own a malicious website with which he/she can trick people into giving access to their data.

3. Conclusion

The aim of this subject was to see how we can avoid Botnets attacks and what lessons we can learn from this to protect our private data.

Once infected with a Botnet you can't escape it that easily, especially if you're not an experienced person, it takes time and one or more countermeasures to deal with it.

Blacklisting is not a direct counter-measure but it's perceived as a supporting process which provides input for further technical means of resistance. Blacklists are used to block the traffic from included addresses and mark websites with suspicious activities.

The distribution of fake credentials is a countermeasure that targets the Botnet profitability by attacking the business model. The most common application is identity theft through which the attacker is stealing credentials and credit cards records.

Another countermeasure is "Port-blocking" and is a preventive measure that can be applied by the Internet Service Providers to reduce the amount of spam mails that go through their network.

The concept of "Walled Gardens" has the goal of protecting the customer and other Internet users that have the same ISP from further damage, by intercepting and isolating outgoing connections from an infected host.

There are so much more ways of detection and countermeasures used for different types of bots, but what these presented ones can tell us is that getting rid of a Botnet requires time and a lot of methods combined as it tends to be unpredictable. The lessons that we can learn from these attacks is that we shouldn't trust our data to anyone that's not credited and to avoid downloading and opening suspicious files from emails or the web. For better protection everyone should consider the use of an Antivirus software and Firewall as they can help us avoid many of the Internet threats.

4. References

- Schiller, C., Binkley, J., Bradley, A., Cross, M., Evron, G., Harley, D. and Willems, C. (2007). *Botnets, The Killer Web App*. Syngress Publishing, Inc., p.30.
- Álvarez Cid-Fuentes, J., Szabo, C. and Falkner, K. (2018). *An adaptive framework for the detection of novel botnets*. [online] sciencedirect.com. Available at: https://www.sciencedirect.com/science/article/pii/S0167404818309805.
- Wang, T., Lin, H., Cheng, W. and Chen, C. (2018). *DBod: Clustering and detecting DGA-based botnets using DNS traffic analysis*. [online] sciencedirect.com. Available at: https://www.sciencedirect.com/science/article/pii/S0167404816301250.
- Chen, C. and Lin, H. (2018). Detecting botnet by anomalous traffic*. [online] sciencedirect.com. Available at: https://www.sciencedirect.com/science/article/pii/S221421261400026X.
- Plohmann, D., Gerhards-Padille, E. and Leder, F. (2011). Botnets: Measurement, Detection, Disinfection and Defence. pp.79, 80, 86, 87.
- Chadd, A. (2018). DDoS attacks: past, present and future. [online] sciencedirect.com. Available at: https://www.sciencedirect.com/science/article/pii/S1353485818300692.
- Sadeghian, A. and Zamani, M. (2018). Detecting and preventing DDoS attacks in botnets by the help of self triggered black holes - IEEE Conference Publication. [online] Ieeexplore.ieee.org. Available at: http://ieeexplore.ieee.org/abstract/document/6924468/.