Distributer denial of service/BotNet attacks

GROUP 5

ANTONIU BEATRICE w1688177@my.westminster.ac.uk
BECHI DENIS w1680643@my.westminster.ac.uk
DETYNA-BIERNAT WIKTOR w1691541@my.westminster.ac.uk

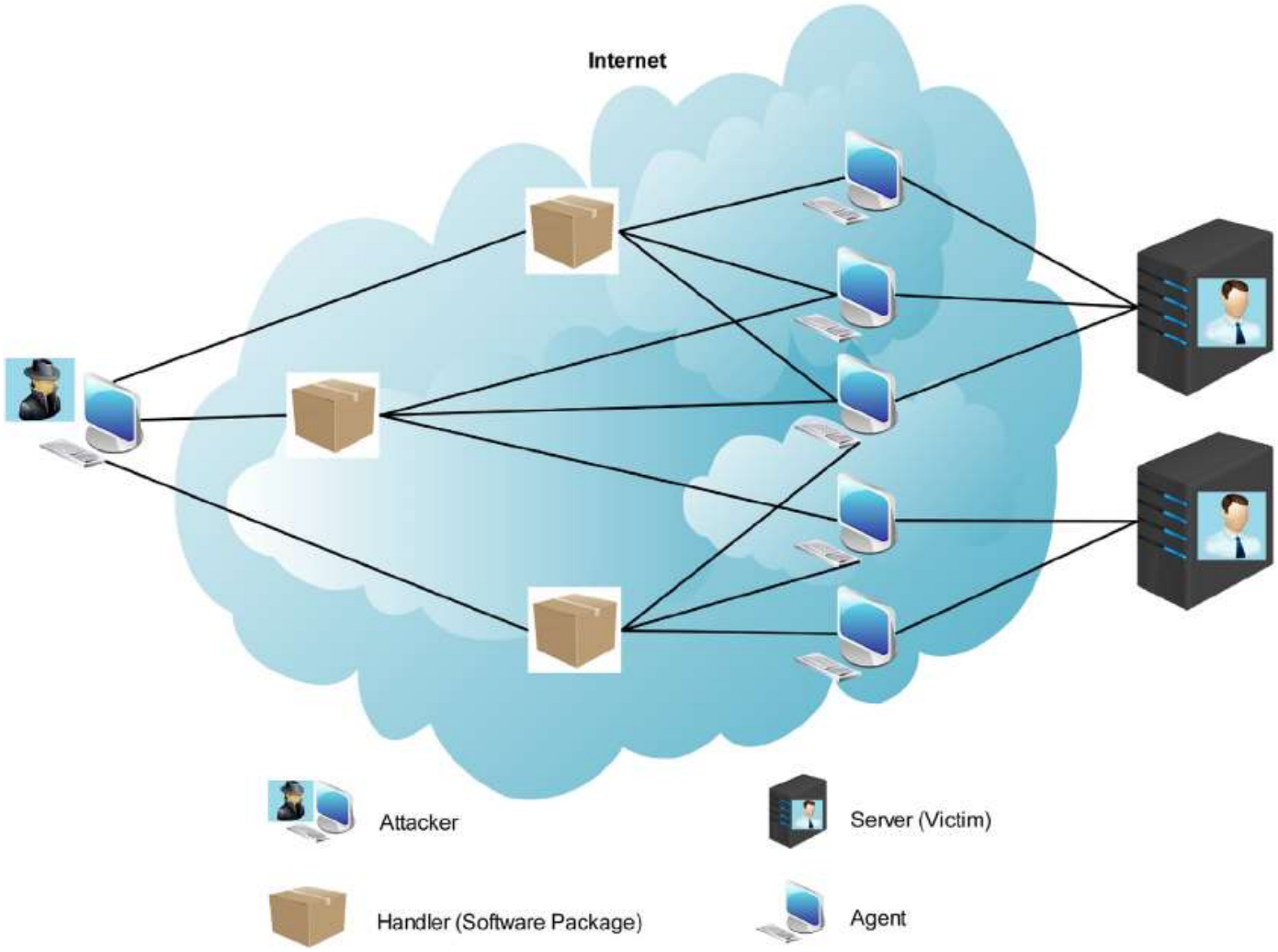
INTRODUCTION

WHAT MAKES A BOT NET A BOTNET?

Botnets are networks of illegally controlled computers typically employed for malicious activities(Grizzard et al., 2007). These networks are created by infecting a large number of computers with malware by means of operating system vulnerabilities, USB drives, or malicious web sites.

- A botnet is the melding of many threats into one. The typical botnet consists of a bot and one or more bot-clients.
- Botnets with hundreds or a few thousands of bot-clients are considered small botnets.
- A typical botnet consists of four phases: infection, command and control connection, attack and post-attack.
- The clients in a botnet must be able to take actions on the client without the hacker having to log into the client's operating system.
- Once a victim's computer is infected, the botnet software allows an attacker to take control and carry out malicious activities such as e-mail spamming or distributed denial-of-service attacks.

If a collection of computers meet these criteria it is a botnet.


Internet
Attacker
Server (Victim)
Handler (Software Package)
Agent

Does the Internet of Things pose new threats to our private data?

Botnets have become a common channel for developing cybercrimes.

The growth of botnets has attracted a lot of attention on the security research and research community. According to the research reports (McAfee, 2012; Trend Micro, 2009), botnets have played a big dangerous threat to the Internet, responsible for various malicious activities from distributed denial of service (DDoS) to spamming, phishing, information harvesting and identity theft.

In February 2018, the first documented native IPv6 DDoS attack occurred, originating from around 1,900 native IPv6 hosts on more than 650 different networks. The attack demonstrates the innovative methods being used by hackers to corrupt systems and highlights things to come, leaving businesses with yet another challenge on their hands. In addition, security researchers have recently raised the alarm about a huge new Internet of Things (IoT) botnet discovered last year called Satori, the successor to the Mirai DDoS botnet. While the malware behind Mirai was sophisticated, Satori represents a major leap in capabilities, meaning even low-level cyber-criminals could launch a potentially devastating attack, with little effort.

- **Spamming**

Spam which is also known as junk mail is a type of message that is sent directly or indirectly from a sender to people that they do not have any relationship with. The spam email also might carry infected attachments.

- **Sniffing Traffic and Key Logging**

Bots are able to sniff the data that victim transmit over the network. These data can be a text, a voice message, an image or even a video.

Bots also might have the key logging service.

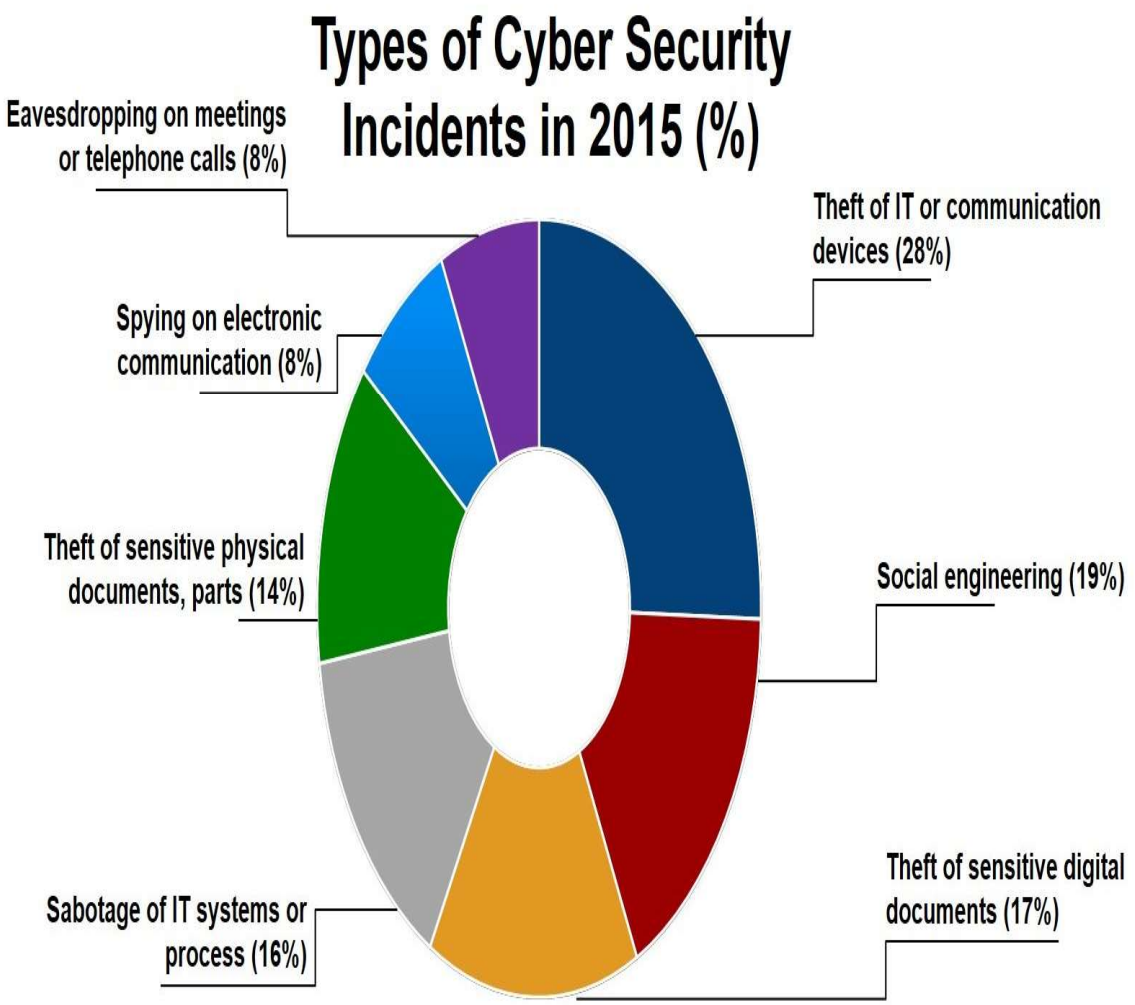
- **Hosting of Illegal Software on Files**

Since the attacker has full control over the large number of hosts using bots, he might use these hosts to share cracked software or movies that are copied and are illegal to distribute. Later if the victim host gets cut, all the blame will go to the victim for illegal distribution of copyrighted materials.

- **Click Fraud**

Some Online Advertisement Campaign like “pay-per-click”, only payoff for clicks from unique IPs on the advertisement. A malicious person may run a website including a PPC advertisement and negotiate with a botnet service provider to buy bulk click from him.

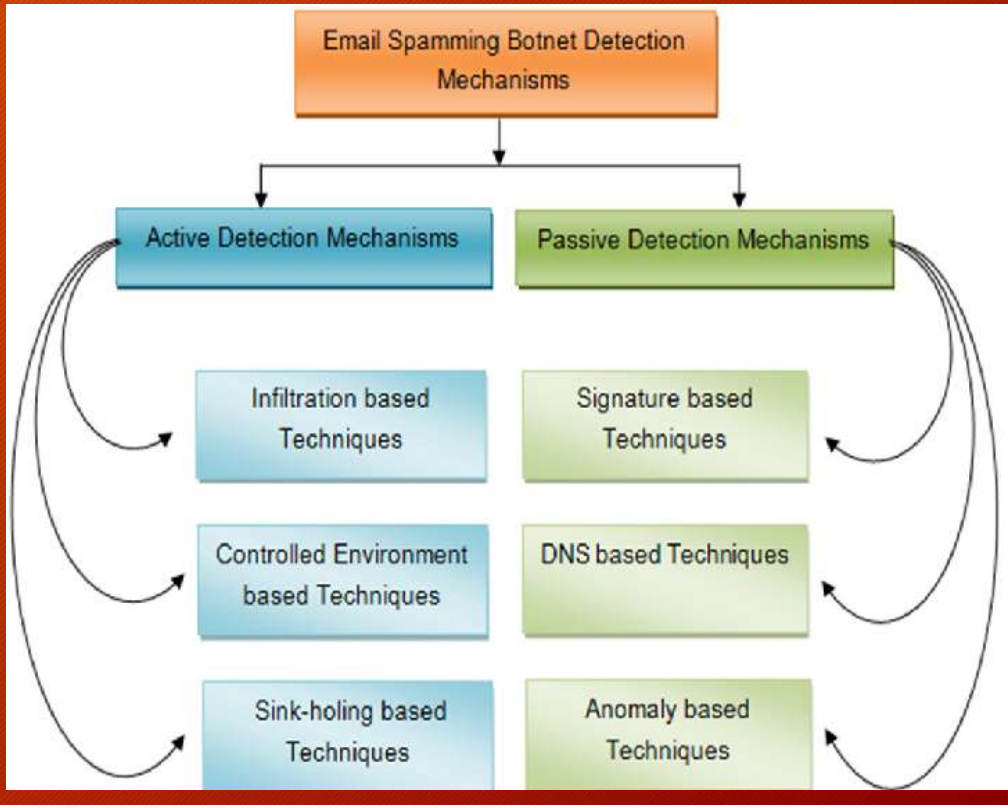
IoT ONE Index: Top 7 Cyber Attacks in 2015



Are there methods to detect DDoS attacks?

The problem of developing effective schemes for detecting botnet activity has attracted significant attention in the network security field(Silva et al., 2013).

1. Signature-based methods provide a relatively straightforward means of identifying botnet activity. However, since they are based on historical botnet patterns, they invariably fail to detect new botnets with a different communication behaviour. While this problem can be resolved by constantly updating the signature database, the associated data analysis task greatly increases the processing cost and reduces the overall performance efficiency (Liu et al., 2009).
2. Anomaly-based techniques perform botnet detection by identifying network traffic anomalies. However, anomaly-based detection methods fail if the communications are encrypted (Silva et al., 2013).
3. DNS-based techniques analyse the DNS traffic generated by botnets.



CONCLUSION

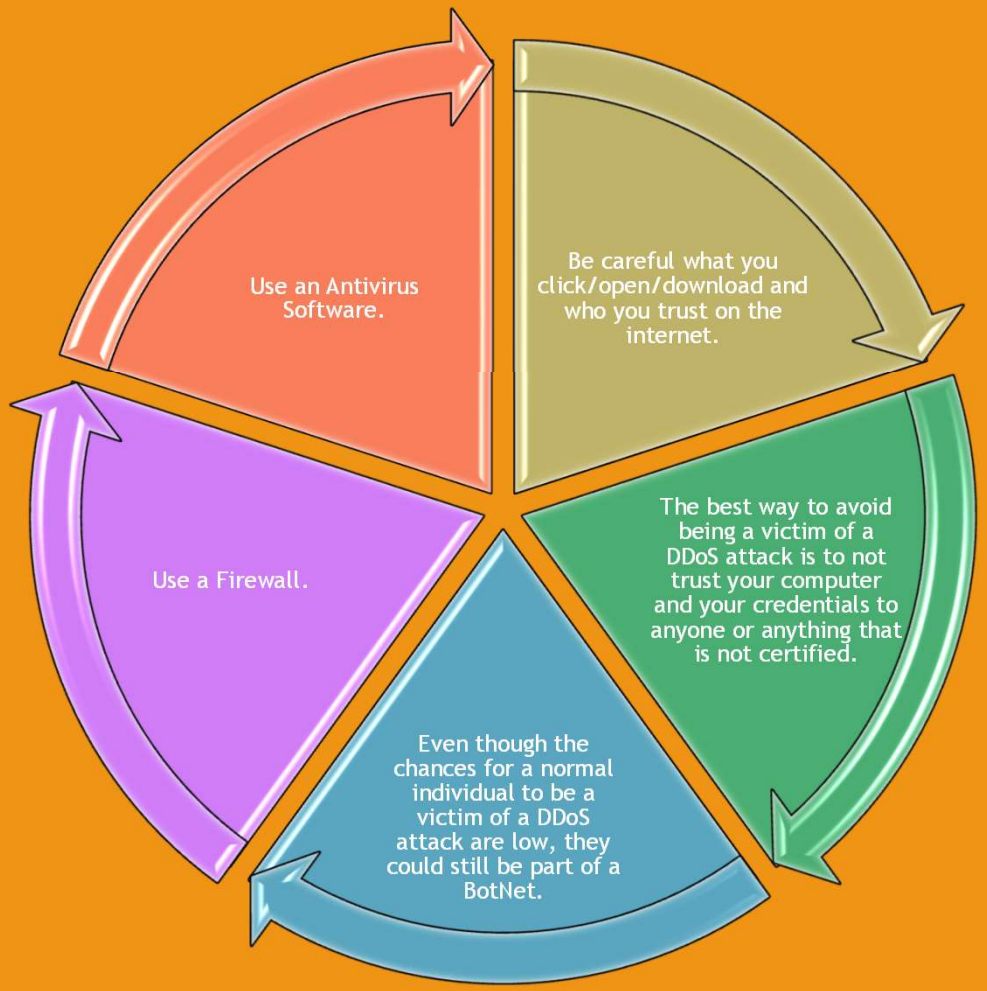
How can the DDoS/BotNet attacks can be avoided?

Although there are lot of ways to detect and get rid of a BotNet, it might take an experienced person to deal with it.

These are a few counter-measures to help eliminate or reduce the threat:

- Blacklisting is not a direct counter-measure against botnets. Instead, it should be perceived as a supporting process which provides input for further technical means of resistance. One use of blacklists is to block all traffic from included addresses. Another application of a blacklist consists of a collection of URLs which can be used by search engines, or within a browser, to filter or mark websites with suspicious or proven malicious contents.
- The distribution of fake credentials is not only a purely technical counter-measure but also targets the botnet's profitability by attacking the underlying business model. A common botnet application is identity theft.
- 'Port blocking' is a preventive measure that can be applied by ISPs to reduce the amount of spam mails traversing their network. As more than 87% of all email is reported as spam, mitigation of this threat is desirable.
- Walled Gardens: the concept has the goal of protecting an ISP's (internet service provider) customers and other Internet users from further damage, by intercepting and isolating outgoing connections from a detected infected host.

CRITICAL EVALUATION



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/.