* **What makes a botnet a botnet?**

1. 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.
2. Many clients must be able to act in a coordinated fashion to accomplish a common goal with little or no intervention from the hacker.

* If a collection of computers meet this criteria it is a botnet.
* 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.

***Source: Botnets, The Killer Web App by Craig Schiller; James R. Binkley; Anthony Bradley; Michael Cross; Gadi Evron; David Harley; Chris Ries; Carsten Willems.***

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. 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. Upon infection, and to remain undetected, bots typically update themselves, disable antivirus applications, block DNS lookups to certain domains, and download and run other types of malware.

***Source: An adaptive framework for the detection of novel botnets by Javier Álvarez Cid-Fuentes, Claudia Szabo, Katrina Falkner***

The problem of developing effective schemes for detecting botnet activity has attracted signiﬁcant attention in the network security ﬁeld. Depending on the particular method used, Botnet detection schemes can be broadly classiﬁed as either signature-based or anomaly-based (Silva et al., 2013). Schemes of the former type extract pattern information from the monitored trafﬁc, mark the signature, and register it on a blacklist.

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).

Anomaly-based techniques perform botnet detection by identifying network trafﬁc anomalies. Goebel and Holz (2007) presented a technique for detecting IRC-based botnets based on an evaluation of well-known IRC channel name patterns. Lu and Ghorbani (2008) developed an IRC botnet detection scheme based on anomalies in the request response time. Gu et al. (2007) proposed a passive botnet detection system designated as BotHunter, in which networking activities were associated with particular state-based infection models in accordance with their dialogue behaviour. However, since the models are predeﬁned, Guet al. (2007) proposed a passive botnet detection system des-ignated as BotHunter, in which networking activities wereassociated with particular state-based infection models in ac-cordance with their dialogue behavior. However, since themodels are predeﬁned, BotHunter is unable to detect malwareswhose behaviors differ from those of existing bots. BotSniffer(Gu et al., 2008) exploits the fact that all bots belonging to thesame malware respond to a command from the botmaster inthe same way. BotMiner (Gu et al., 2008) improves the detec-tion performance of BotSniffer by employing a cross-clustercorrelation technique to identify hosts which share both similarcommunication patterns and similar malicious activities.

Stone-Gross et al. (2009) used a DNS-based detection approach to identify a new class of botnetknown as Domain Flux botnets, in which the bots generatenumerous domain names using a DGA and then attempt toestablish communications with a subset of them. The sameauthors used a similar approach to identify Torpig attacks, inwhich the bots take common words used in Twitter searchesas seeds to generate new domain names e v ery day.

**Source: Bod: Clustering and detecting DGA-based botnets using DNS trafﬁc analysis**

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. Botnet becomes one of the major threats on the Internet.

Botnet becomes one of the major threats on the Internet. Some researchers analysed botnet behaviours to understand the architecture and the capabilities of bots.

**Source: Detecting botnet by anomalous traffic\* by Chia-Mei Chen\*, Hsiao-Chung Lin**

Blacklisting is not a direct countermeasure 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 countermeasure but also targets the botnet‘s profitability by attacking the underlying business model. A common botnet application is identity theft. Profit is created by stealing credentials or credit card records.

‘Port blocking‘ is a preventive measure that can be applied by ISPs to reducing the amount of spam mails traversing their network. As more than 87% of all email is reported as spam [6], mitigation of this threat is desirable.

The Border Gateway Protocol (BGP) is widely used throughout the Internet and has consequently become the predominant technology for decisions on the routeing of network traffic. BGP is used to maintain the Internet routeing table, which is organised in chunks of IP addresses, and ensures the accessibility of so-called autonomous systems (AS), for instance ISP networks.

The concept of a ‘walled garden’ has the goal of protecting an ISP‘s customers and other Internet users from further damage, by intercepting and isolating outgoing connections from a detected infected host.

**Source: Botnets: Detection, Measurement, Disinfection & Defence by ENISA**

As DDoS attacks have gained traction across the cyber landscape, the variety of threats has also expanded, bringing to light new methods and motives. In February this year, the first documented native IPv6 DDoS attack occurred, originating from around 1,900 native IPv6 hosts on more than 650 different networks. The total number of possible IPv6 addresses is more than 7.9x1028 times as many as IPv4, making a considerably greater attack volume possible. 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. With the stakes higher than ever before and as hackers show no signs of retiring from cybercrime anytime soon, it is essential that businesses understand exactly how to detect and protect themselves from DDoS threats that could be lurking just around the corner.

**Source: DDoS attacks: past, present and future by Anthony Chadd, Neustar**

A Botnet can be used for launching a DDoS Attack. Since if a DDoS attack happens from a limited range of computers it will be very easy to black list the IP address of those computers and track them down, therefore attackers need to have a high speed internet with huge amount of bandwidth. An Attacker by use of Botnet can control a large number of infected host computers and order them to send connection requests to the target host. Since each computer uses its own internet, bandwidth and IP, then it cannot be suspicious for the target host firewall. When all these malicious requests come from different machines from all around the world in the same time, due to the fact that the target host is not able to handle high amount of requests in the same time, it becomes unavailable.

• 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 sender [10]. In other words, it is an unwanted message which most of the time sent for advertisement goals. In case of spamming the protection systems inside the email provider can easily detect and ban the IP address of spam sender but if Spams sent from a Botnet, the IP address of each spammer will be different, because each Bot has its own IP and they can easily bypass the spam filters [11]. The spam email also might carry infected attachments, if the recipient opens the attachment it will add him/her computer as a new node to the Botnet.

• Sniffing Traffic and Key Logging

Bots are able to sniff the data that victim transmit over the network. These data can be a text, voice message, image or even a video. The hacker will use this information to learn more about victim habits or gather victim private information for further social engineering attacks. Bots also might have the key logging service. This service will collect all the keys pressed by the user on the keyboard and hacker can filter the range of captured keys to keys that pressed in special field like username, password and credit card number to avoid capturing high amount of useless keys and information. Hacker by the help of this service can easily steal all the critical information of the victim such as username and password of accounts and all credit cards information that needed to be used for an online shopping.

• Identity Theft

Attacker might use the gathered information at the key logging and sniffing process to make fake IDs and uses them for criminal activities which victim will be responsible for those actions.

Another technique of Identity theft that used by botnets is sending phishing emails which invite users to a fake webpage for collecting their private information such as username, passwords and credit card information.

The attacker may not use this information directly for making fake IDs, however instead he might sell these harvested information to a third party criminal for a good price.

• Hosting of Illegal Software on Files

Since the attacker has full control over large number of host using bots, he might uses these hosts to share cracked software's or movies that are copied and are illegal to distribute. Later if the victim host get cut, all the blames will goes 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 IP's on the advertisement [12]. A malicious person may run a website including a PPC advertisement and negotiate with a botnet service provider to buy bulk click from him. Botnets which are connected from different IP addresses around the world can click on these advertises and make high amount of income for the website owner. The income of advertisement is much higher than the rent of the botnet which makes it a profitable crime.

• Manipulating Online Polls

Online pools and votes use to make big decision. Therefore to avoid repetition in votes they just accept one vote from each unique IP address. The botnet is able to uses it's nodes with different IPs to vote for a specific option and change the result of voting for the benefit of a third party.

**Source: Detecting and preventing DDoS attacks in botnets by the help of self triggered black holes**