Abstract

Botnets are the most common types of threats and often perceived as crucial in terms of national security. Botnet is a network created by the cyber-criminal or a hacker to attack a system with the help of a large number of private computers. Threat modelling of botnet.

For instance, a botmaster executes a DDoS (Distributed Denial of Service) attack using Command and Control Center (C & C) on web server which leads to downtime.

Consequently, effects Availability in a CIA triad. Moreover, there is a huge loss of revenue and user traffics for the companies.

So, there is a need to build well-designed cyberspace model that enables to construct an experimental environment whereby it allows for the analysis of botnet characteristics, testing its resistance to various events.

Thus, this project focuses on threat modelling of botnet-based attacks using attack trees and vectors. Mitigation techniques to prevent botnet attacks are also presented
Using STRIDE, a cyber-model is proposed that constitute vulnerabilities associated with the topology of botnets (centralized or de-centralized).

Prevention, detection, and mitigation of botnet based cyber-attacks are presented in the model.

Vector constitutes

(i) Topology of botnet
(ii) Actors in the cyber-space
(iii) Cyber threats that may occur E.g., Worms
(iv) Methods of attacking mechanisms E.g., DDoS Attack using C&C
(v) Security mechanisms to prevent attacks E.g., Firewall

Literature Review (Draft):

The Spamhaus Project (2019) found that there is an extensive increase of 71.5% of botnet Command & Control Centers for the past two years deducing that there is a rapid increase ofbbbotnet-based attacks in recent times.

The researchers of the Psamhaus Project (2019) found that Emolet and TrickBot malspam campaigns and infections rise drastically.

Polly and Houssain (2019) estimated that approximately 70% of botmasters are influenced by profit since it requires low investment. To design a good cyber-space model, there is a need to analyze various botnet models based on their network topologies such as centralized or decentralized as described in Rafal, Marcin, and Tarpata (2017).

In a centralized botnet network may consists of Command and Control Center (C & C), to issue command over the zombies in the entire network. On the other side, decentralized botnet network operates in a peer-to-peer communication over the network.

botnet-based attacks

To mitigate botnet-based attacks, the distribution or spreading methods of bots that includes computer worms, email spam, warez are to be analyzed as stated in Rafal, Marcin and Tarapata (2017). Some botnet-based networks also follow a random C & C model for attacking webservers as stated by Trend Micro White Paper (2006).

The architecture of botnet-based DDoS attacks is usually of three types, the agent handler, web-based architecture, and Internet Relay Chat (IRC) architecture as described by Esraa, Gupta and Shankar (2012).

Moreover, there is a need to consider lifecycle framework of botnet models which are demonstrated using different stages like Conception, Recruitment, Interaction, Marketing and Execution (CRIME) is Polly and Houssain (2019).

Polly and Houssain (2019) also considered different botnet models like epidemiological, machine learning, stochastic, game theory, NP Bayesian, graph, and economic models, these are useful to propose a pertinent cyber-space model.

Now, a cyber-space model is proposed by constructing a vector with variables like network topology, actors, threats, attacking methods and mitigation techniques.

STRIDE model approach

It is followed to defend DDoS attacks based on botnets using the reference of security analysis made by Sakshit Janitla and Kornchawal Chaipah (2016).

The hybrid mechanism proposed by Sakshit Janitla and Kornchawal Chaipah (2016) is useful in creating a cyber-space model that prevents or mitigates DDoS attacks.

For an experimental evaluation of the proposed cyberspace model, a performance analysis is performed on the webserver before the botnet-based attack and after executing a DDoS attack on a virtual network.

Performance metrics

They are used for measuring the impact of DDoS attack by considering Quantitative and measurement at different attacking strengths and measuring service degradation using throughput, response time as stated by Monika, Gurvinder Singh and Kuldip Singh (2009).

This result in a performance evaluation citing a decrease in performance of webserver when a botnet-based attack is launched. Further, the performance analysis is performed after the cyber-space model is implemented.

The result obtained to serve as a shred of evidence to substantiate the practical implementation of the proposed threat model.

Note:
Professor, I'm still reading other papers, so will update literature review in a coherent manner after reading the remaining papers.

References:

[1] Modeling and simulation of botnet based cyber-threats, Rafal Kasprzyk, Marcin Paz, Zbigniew Tarapata (2017)
https://www.researchgate.net/publication/320204415_Modeling_and_simulation_of_botnet_based_cyber-threats/link/59df91cd0f7e9b2dba8393d9/download
[2] An Analysis of Botnet Models, Polly Wainwright, Houssain Kettani (2019)
https://www.researchgate.net/publication/332082920_An_Analysis_of_Botnet_Models
[3] Botnet Threat Report 2019, The Spamhaus Project
https://www.spamhaustech.com/custom-content/uploads/2020/04/2019-Botnet-Threat-Report-2019-LR.pdf
[4] Botnet-based Distributed Denial of Service (DDoS) Attacks on Web Servers: Classification and Art, Esraa Alomari, B.B Gupta, Shankar Karuppayah (2012)
https://research.ijcaonline.org/volume49/number7/pxc3880724.pdf
[5] Performance Analysis of Web Service under DDoS Attacks, Monika Sachdeva, Gurvinder Singh, Kuldip Singh (2019)
https://www.researchgate.net/publication/224398665_Performance_Analysis_of_Web_Service_under_DDoS_Attacks
[6] A security analysis of hybrid mechanism to defend DDoS attacks in SDN, Sakshit Janitla and Kornchawal Chaipah (2016)
https://core.ac.uk/reader/82088498
[7] Taxonomy of Botnet Threats (2006), A Trend Micro White Paper
https://sites.cs.ucsb.edu/~kemm/courses/cs595G/TM06.pdf
[8] Botnets: Detection, Measurement, Disinfection & Defence (ENISA)
https://www.enisa.europa.eu/publications/botnets-measurement-detection-disinfection-and-defence/at_download/fullReport
[9] Business Model of a Botnet
https://arxiv.org/pdf/1804.10848.pdf
[10] Your Botnet is My Botnet: Analysis of a Botnet Takeover
https://www.isg.rhul.ac.uk/sullivan/pubs/torpig-ccs09.pdf
[11] A Multifaceted Approach to Understanding the Botnet Phenomenon
http://www.cs.jhu.edu/~fabian/papers/botnets.pdf
[12] Modelling DDoS and Defences
http://www.casos.cs.cmu.edu/publications/papers/chen_ddos.pdf