CSE 363: Computer Security

Final Project Proposal

Authors:

Cody Johnston - *cody.johnston@student.nmt.edu*
Cole Johnson - *cole.johnson@student.nmt.edu*
Colin Grandjean - *colin.grandjean@student.nmt.edu*
John Runyon - *john.runyon@student.nmt.edu*
New Mexico Institute of Mining and Technology
Socorro, NM 87801, USA

Date: March 3, 2025

Purpose and Outline of Project

A botnet (the combination of the words robot and network) is a group of network enabled malware infected. Bots, the infected devices, are controlled by a central server or servers, often called the "bot-herder" or the "command and control server" [4]. A botnet can be used for a wide variety of malicious activities. From DDoS attacks to data theft, botnets can interfere with computer information systems in a variety of ways and are worthy of studying and considering mitigation techniques. Our paper will focus on discussing the threats botnets pose, the mitigation techniques currently implemented, and later we will implement a basic botnet to demonstrate attacks and mitigation techniques.

Outline of Project

Here is what we would tentatively like to cover in each section of our paper:

(a.) Introduction

- (a.) What are botnets?
- (b.) Examples of botnets
- (c.) Famous cases of botnet attacks

(b.) Taxonomy of Botnets

- **(a.)** Architecture / Design
- **(b.)** Communication Methods
- **(c.)** Purpose

(c.) Attack Vectors

- (a.) Vulnerabilities
- (b.) Phishing
- (c.) Worm-Like
- (d.) External Devices

(d.) Mitigation Techniques

- (a.) Firewalls

(b.) Intrusion Detection Systems (IDS)

(c.) Challenge and Response Tests

(e.) Experimentation

(a) Existing botnet frameworks

(b) Developing a basic botnets

(c) Implementing mitigation techniques (if time permits)

Taxonomy of Botnets

Botnets can be constructed in a number of ways and fulfill many different purposes for an attacker. They can either be centralized, using a client-server model, decentralized, using a peer-to-peer model, or a hybrid approach that is a combination of centralized and decentralized architectures [1].

Attack Vectors

Botnets exploit various attack vectors to infect devices and expand their network. The most common methods that botnets use are exploiting vulnerabilities, phishing, worm-like propagation, and using external devices [3]. Botnets exploit vulnerabilities such as unpatched software, misconfigurations, and security loopholes found within operating systems, applications, or IoT devices [1].

Mitigation Techniques

There any a myriad of different techniques that try to mitigate the damage caused by botnets, or limit their spread altogether. We would like to focus on a few different techniques: firewalls, intrusion detection systems [2], and challenge response tests.

Experimentation and Results

We first plan to look into existing botnet frameworks to examine their methods and features. After research into frameworks, we plan to build a simulated botnet, with various bot devices running in containers. Using a modularized approach we can change the purpose of the botnet dynamically to explore the differences. We plan to compare botnet communication and architecture methods by running a set of tasks

for the different methods. If time permits we plan on testing different mitigation techniques.

Conclusion

Our project will explore botnets in a variety of different contexts. We will attempt to approach the subject both from a research-based approach, creating an overview of botnets as they relate to computer security, and from an experimental approach by attempting to implement a basic version of a botnet.

References

[1] Frank Antonucci and MD Minhaz Chowdhury. "Botnets as the Modern Attack Vector". In: *2022 IEEE World AI IoT Congress (AIIoT)*. 2022, pp. 585–590. DOI: 10.1109/AIIoT54504.2022.9817360.

[2] Stefan Axelsson. "Intrusion Detection Systems: A Survey and Taxonomy". In: (Apr. 2000).

[3] Morey J. Haber, Brian Chappell, and Christopher Hills. "Attack Vectors". In: *Cloud Attack Vectors: Building Effective Cyber-Defense Strategies to Protect Cloud Resources*. Berkeley, CA: Apress, 2022, pp. 117–219. ISBN: 978-1-4842-8236-6. DOI: 10.1007/978-1-4842-8236-6_6. URL: https://doi.org/10.1007/978-1-4842-8236-6_6.

[4] Simon Heron. "Botnet command and control techniques". In: *Network Security* 2007.4 (2007), pp. 13–16. ISSN: 1353-4858. DOI: https://doi.org/10.1016/S1353-4858(07)70045-4. URL: https://www.sciencedirect.com/science/article/pii/S1353485807700454.