ENCODERSPRO
An AKTU-Incubated CyberSecurity Company

Scope of Work

Modular Botnet Simulation and Analysis

Submitted in partial fulfillment of the requirements

By

Team - अनिर्वचनीय

Project Duration:

28/6/2025 – 11/7/2025

Abstract

This report details the design and implementation of a modular botnet simulation within a secure, virtualized lab environment. The project includes the development of a web-based Command and Control (C2) dashboard, modular Python-based malware bots, and a target server to test post-infection behaviors like keylogging, scanning, and DDoS attacks. The primary goal was to understand malware behavior, botnet communication, and forensic techniques within the bounds of ethical containment.

1. Introduction

In the rapidly evolving field of cybersecurity, botnets represent one of the most persistent and dangerous threats to organizational and personal digital assets. A botnet is a network of compromised machines (bots) that are remotely controlled by an attacker, typically via a centralized or decentralized Command and Control (C2) infrastructure. These networks can be used for various malicious activities, including DDoS attacks, data theft, credential harvesting, and spreading malware.

This project, titled "Modular Botnet Simulation with Web-Based C2", is a hands-on simulation designed to understand how botnets operate from both an attacker's and defender's perspective. The focus of the project is to develop modular botnet clients for both Linux and Windows using Python, and simulate real-world cyberattack behaviors within a controlled lab environment. The bots communicate with a custom-built web-based C2 server, allowing command issuance and data retrieval through secure HTTP protocols.

Additionally, the project integrates network traffic analysis using tools like Wireshark to examine the communication patterns between bots and the C2 server. This provides deeper insight into how malicious traffic can be detected and analyzed using modern intrusion detection techniques.

By simulating such environments, the project serves both offensive and defensive research purposes, offering valuable knowledge for understanding, detecting, and mitigating botnet threats within enterprise networks.

2. Background

Botnets are automated malware agents capable of executing commands from a centralized controller. Historically, they have been used for various attacks, including distributed denial of service (DDoS), data theft, and unauthorized surveillance. By replicating such a system in a lab environment, students gain hands-on experience with both offensive and defensive cybersecurity tactics.

3. System Architecture and Methodology

The project architecture includes

- **C2 Dashboard**: A web interface built using Flask to manage, monitor, and issue commands to bots.
- **Bot Clients**: Python-based agents capable of performing tasks such as keylogging, network and port scanning, data stealing, spyware operations, brute-force attacks, and DDoS attacks in both Linux and Windows environments.
- **Target Server**: A local Ubuntu-based server used to test and simulate attacks.
- **Virtualized Environment**: Using VMware with systems like Kali Linux to ensure safe and isolated simulation.

Communication is facilitated over HTTP, with bots polling the C2 server for instructions. Data is logged, and network traffic is monitored using Wireshark and tcpdump.

4. Implementation

4.1 C2 Dashboard

The dashboard includes routes for bot registration, command assignment, and activity logging. A simple UI allows team members to issue commands and monitor bot status.

4.2 Bot Modules:

- **Keylogger**: Captures keystrokes and sends logs to C2.
- **Network and Port Scanner**: Scans the local subnet to identify active IP addresses on the LAN and detects open ports and running services on the local system and active addresses found.
- **DDoS Module**: Launches HTTP flood attacks by sending a large volume of HTTP requests to overwhelm the target server.
- **Spyware:** Monitors user activity, captures screenshots, and logs sensitive information from the target system without user awareness.
- **Stealer:** Extracts and exfiltrates stored credentials, browser history, saved passwords, and other sensitive data from the infected system.
- **Brute-force Module**: Simulates password-guessing attacks on HTTP, SSH and FTP services to test weak or default login credentials.

4.3 Virtual Machines

One attacker machine (Kali Linux serving as the C2 server), one Linux machine, and one Windows machine were infected. The web server remains uninfected and is used solely for attack demonstration purposes.

5. Experimental Setup

- **Environment**: Configured on VMware using Internal Private Network.
- **Traffic Capture**: Wireshark and tcpdump are used to analyze bot-C2 communication.

6. Analysis and Discussion

This project intends to simulate the behavior of a modular botnet in a controlled environment to better understand its technical operations, communication patterns, and forensic impact.

A major component of the analysis will involve capturing and studying the network traffic between the bots and the C2 server. Tools like Wireshark will be used to inspect these communications, helping us identify traffic patterns, command structures, and potential indicators of compromise. This will aid in understanding how botnets interact with their C2 infrastructure and how such behavior might be detected or mitigated.

We also plan to investigate how specific modules such as keyloggers, DDoS tools, and network scanners leave forensic artifacts on the infected systems. This includes identifying changes such as created files, system log entries, background processes, and modified configurations.

We anticipate encountering challenges such as maintaining stable communication with multiple bots, handling concurrent execution of payloads, and isolating relevant traffic and system data for analysis. However, addressing these challenges is expected to provide valuable insights into malware development, detection techniques, and system-level forensic analysis.

All activities will be conducted within isolated virtual machines to ensure safe and ethical experimentation. No code or behavior will be allowed to interact with external systems or networks. The entire project will follow strict cybersecurity research guidelines and is intended solely for educational and research purposes.

7. Conclusion and Future Work

This project is designed to simulate a modular botnet operating in a controlled virtual environment, using both Linux and Windows based bot clients. It aims to provide hands-on experience with malware behavior, command-and-control (C2) communication protocols, persistence techniques, and network forensic analysis.

The intended outcome is a functional simulation that demonstrates the core functionality of a botnet from infection to remote command execution, along with meaningful insights into botnet detection and monitoring. By the end of this simulation, the team expects to gain both practical skills in malware engineering and a foundational understanding of cyber defense strategies in response to botnet threats.

As part of future expansion, the project could be extended to incorporate

- Encrypted communication between bots and the C2 server.
- Cross-platform compatibility and evasion techniques.
- Machine learning-based anomaly detection to identify botnet behavior.

8. Approval

This Scope of Work is submitted as part of the final project documentation for internal review and evaluation.