GitHub - jgamblin/Mirai-Source-Code: Leaked Mirai Source Code for Research/IoC Development Purposes

By jgamblin

Archived: 2026-04-05 17:15:13 UTC

🔧 Requirements

Before building and running this code, ensure you have the following installed on a **Linux host**:

- `gcc` - GNU Compiler Collection
- `golang` - Go programming language
- `electric-fence` - Memory debugging library
- `mysql-server` - MySQL database server
- `mysql-client` - MySQL database client
- `build-essential` - Essential build tools
- `crossbuild-essential-armel` - Cross-compilation tools for ARM

Additional Resources:

- For detailed setup instructions and background information, refer to the original leak post in `ForumPost.txt` or view the formatted version at ForumPost.md.

⚠️ CRITICAL DISCLAIMER

This repository contains the leaked source code of the **Mirai botnet**, originally created to infect IoT devices and launch large-scale DDoS attacks. This code is provided **strictly for cybersecurity research, reverse engineering, malware analysis, and detection development purposes only**.

⚠️ WARNING: Do not use this code to attack or scan any real devices or networks. Unauthorized use is illegal and violates GitHub policy.

🛡️ **SECURITY NOTICE:** The zip file for this repo is being identified by some AV programs as malware. Please take caution.

📋 Table of Contents

📌 About Mirai

Mirai is a malware botnet that infects Internet of Things (IoT) devices using default or weak login credentials. Once infected, these devices are controlled by a command-and-control (CnC) server and can be used to launch DDoS attacks.

This repo is a fork of the original leaked source code and includes components such as:

- The bot (runs on IoT devices)
- The CnC server
- The loader (infects devices)
- Scanning and deployment scripts

📁 Repository Structure

Folder/File	Description
`mirai/`	Core malware source code (bot + CnC server)
`loader/`	Infects vulnerable devices using telnet brute-force
`dlr/`	Possibly supports payload delivery (optional)
`scripts/`	Scripts for building and managing the malware
`ForumPost.txt`	Original forum post by author explaining Mirai
`LICENSE.md`	License as included in original leak (not official)
`README.md`	You're reading it

⚙️ How to Use (FOR LAB RESEARCH ONLY)

> You must use **isolated VMs** or an offline network. Never run this on a real device or public network.

🔧 1. Prerequisites

Install on a **Linux host**:

```
sudo apt update
sudo apt install gcc make build-essential git crossbuild-essential-armel -y
```

🔨 2. Clone the Repository

```
git clone https://github.com/jgamblin/Mirai-Source-Code.git
cd Mirai-Source-Code
```

🔨 3. Build the Bot and CnC

This will:

- Cross-compile the bot for different IoT architectures (MIPS, ARM, etc.)
- Compile the CnC server for your local machine

You can customize the build script and source code paths if needed.

🧪 4. Setup a Test Lab (Recommended)

Create a virtual lab with:

- 1 Ubuntu VM for CnC and loader
- 1 or more OpenWRT/Linux VMs simulating IoT devices

Use Host-Only or Internal Networking mode to keep the lab isolated.

🕹 5. Running Components

- Start the CnC server (mirai/cnc/cnc)
- Run the loader to infect virtual IoT VMs
- Observe communication logs, infection, and payload delivery

✅ Learning Use Cases

You can use this source code to:

- Understand how botnets spread through weak credentials
- Reverse engineer malware behavior
- Write intrusion detection rules (YARA, Snort, Suricata)
- Develop antivirus and botnet defenses

- Study CnC-to-bot protocol and build simulators

❌ Do NOT Use For

- Scanning or infecting real IoT devices
- DDoS attacks
- Deploying the bot to the public internet

Any such use is illegal and against GitHub policy.

📚 References

- Original Leak on Hackforums (2016)
- DDoS Analysis of Mirai by MalwareMustDie
- US-CERT Alert TA16-288A

👨‍💻 Credits

Original Author: Anna-senpai - Original Mirai botnet source code leak (2016)
Note: The original forum appears to be inactive as of now.

🙏 Acknowledgments

Special thanks to Pushpenderrathore for the improved README structure and comprehensive documentation that makes this educational resource more accessible for cybersecurity research.
