UDC 621.391

doi: 10.20535/2411-2976.12024.50-54

ANALYSING MALICIOUS SOFTWARE SUPPORTING DDOS ATTACKS ON IOT NETWORKS

Valerii V. Pravylo, Yevhenii O. Averkiiev

Educational and Research Institute of Telecommunication Systems
Igor Sikorsky Kyiv Polytechnic Institute, Kyiv, Ukraine

Background. With the proliferation of Internet of Things (IoT) networks in the digital age, the risk of cyberattacks, especially DDoS attacks, is also increasing. IoT devices such as smart refrigerators, thermostats, webcams and other Internet-connected home appliances are being targeted by attackers who can use them as part of a botnet to conduct DDoS attacks. These devices often have inadequate network security and are rarely updated, making them vulnerable. DDoS attacks can result in significant losses such as lost revenue, reputational damage and costs to restore services. So, the vulnerability of IoT networks to DDoS attacks and the need to develop effective protection measures is a pressing issue.

Objective. The purpose of the paper is to analyse software that supports DDoS attacks in IoT networks. Provide general recommendations to help improve approaches to defence measures in IoT networks against DDoS-enabled malware.

Methods. Five main DDoS attack models are considered: agent-handler model, reflexive model, IRC-based model, web-based model, and P2P-based model. Three most dangerous software capable of DDoS attacks on IoT networks are analysed: Mirai, XOR.DDoS and Linux.Hydra.

Results. There are many models and methods of DDoS attacks on IoT networks. The most dangerous are Mirai, XOR.DDoS and Linux.Hydra. Each of these software has its own specific characteristics and methods of carrying out attacks. The study also showed that there are several effective measures to counter these attacks, including setting strong passwords, regularly updating software, setting up traffic filters and restricting network access.

Conclusions. Key aspects of DDoS attacks, their models and process steps are considered. The paper focuses on the three most dangerous software used to conduct such attacks and provides recommendations on how to counteract them.

Keywords: *DDoS; IoT; cyberattack; botnet; malware; Mirai; XOR.DDoS; Linux.Hydra; network security; DDoS countermeasures.*

Introduction

In today's digital age, the Internet of Things (IoT) is becoming more pervasive, but with it comes an increasing risk of cyberattacks, especially DDoS attacks. This presentation analyses the software that supports DDoS attacks in IoT networks and strategies to counter them. It also discusses general recommendations for improving IoT networks' defence measures against malware that supports DDoS attacks. First, it is necessary to explain what a DDoS attack is.

Definition of the term "DDoS Attack"

A DDoS (Distributed Denial of Service) attack is a type of cyberattack aimed at overloading a network resource so that it becomes unavailable to legitimate users. This is accomplished by sending a huge number of requests to the target server or network, resulting in a denial of service. A general diagram of a DDoS attack can be seen in Fig.1.

In the context of the Internet of Things (IoT), DDoS attacks are particularly dangerous. IoT devices such as smart refrigerators, thermostats, and webcams are often connected to the Internet and can be used by attackers to create a botnet. These infected devices can generate a huge number of unwanted requests to the target server, causing it to overload and deny service.

Since IoT devices often have weak security and are rarely updated, they become an easy target for attackers. This makes IoT devices vulnerable to DDoS attacks, which can have serious consequences for users and services.

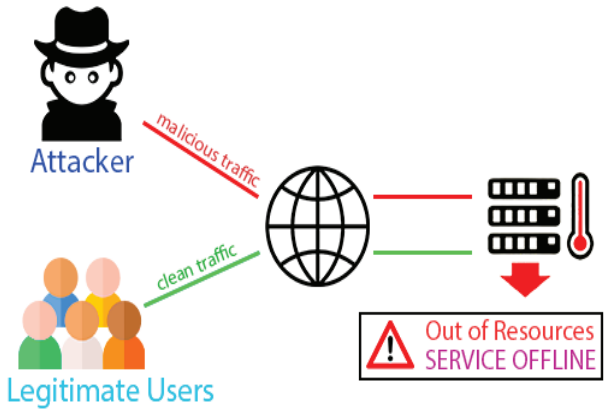

Fig.1 General diagram of a DDoS attack

Stages of formation of DDoS Attack

To successfully conduct a DDoS attack, an attacker performs several key steps. Each of them is important for achieving the ultimate goal of denying service to the target server or network. Let's take a closer look at these steps:

1. Target selection: the attacker identifies a target server, system, or network to attack.
2. Botnet creation: the attacker infects a large number of devices (bots) with malware to form a botnet.
3. Launching the attack: using the botnet, the attacker sends a huge number of requests to the target server. This can be thousands or millions of requests per second.
4. Denial of Service: the server cannot handle all requests due to excessive load, resulting in delays or complete denial of service for legitimate users.

Thus, DDoS attacks can have serious consequences including loss of revenue, reputational damage, and service restoration costs. Therefore, it is important to have a DDoS attack defence strategy that includes prevention, detection, and recovery measures. Once the basic steps have been identified, we need to look at the existing DDoS attack models.

Models of DDoS Attack

As seen in Fig.2, there are five main DDoS attack models:

1. Agent handler model: this model consists of clients, handlers and agents (infected devices). A client is a device used by the attacker to communicate with other elements of the attack. Handlers communicate with agents, learning their state and planning attacks. Agents, usually unnoticed by their owners, perform attacks using minimal system resources.
2. Reflector model: in this model, agents send packets to other, uninfected machines (reflectors) rather than directly to the victim. This hides the source of the attack traffic and amplifies the attack with broadcast IP addresses, which increases the amount of traffic directed to the victim.
3. IRC-based model: similar to the agent handler model, but uses IRC channels for communication between clients and bots. The use of IRC channels makes it difficult to track attacks, provides a high level of secrecy, and does not require the attacker to maintain a list of agents.
4. Web model: similar to the IRC model, but instead of IRC channels, websites are used. This model allows for more effective attack management through complex scripts and encrypted communications. The web-based model provides ease of installation and use, as well as the ability to hide traffic.
5. P2P based model: features a decentralized approach where there are no handlers. Commands are sent to bots through a Peer-to-Peer network, making the system more resilient to failures and making it harder to track attacks. The goal is to destroy all bots to disrupt the P2P network.

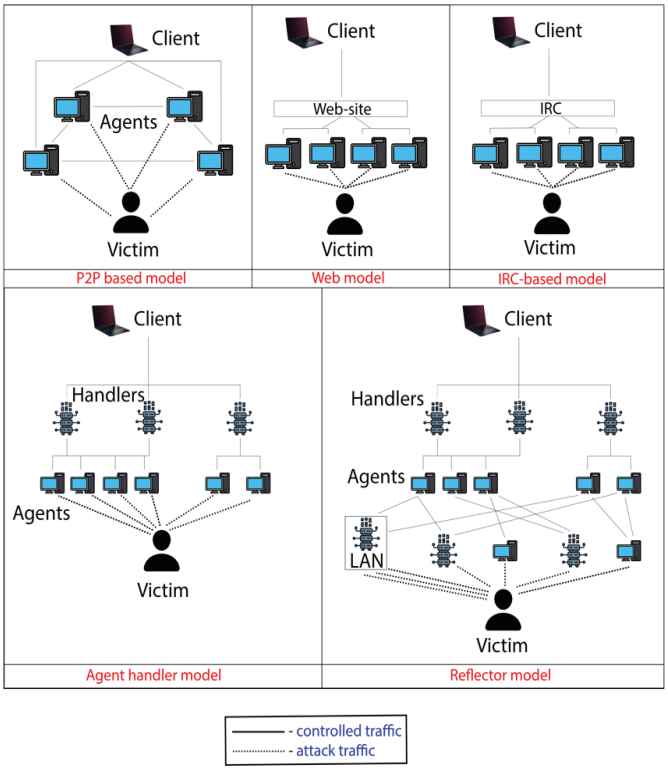

Fig.2 Models of DDoS Attack

Analysing malicious DDoS software

Currently, there are 3 most dangerous pieces of software capable of conducting DDoS attacks on IoT networks.

1. **Mirai**. Mirai is one of the most well-known IoT malware, which was first discovered in 2016. It creates a botnet of infected IoT devices and can perform a variety of DDoS attacks using TCP, UDP, and HTTP protocols.

Mirai's main components are:

- Scanner: detects vulnerable IoT devices.
- Destruction module: eliminates other malware on the device.
- Attacker module: executes DDoS attacks as directed by the management server.
- Reporting server: collects information about vulnerabilities.
- Loader Server: Downloads malware to new devices.

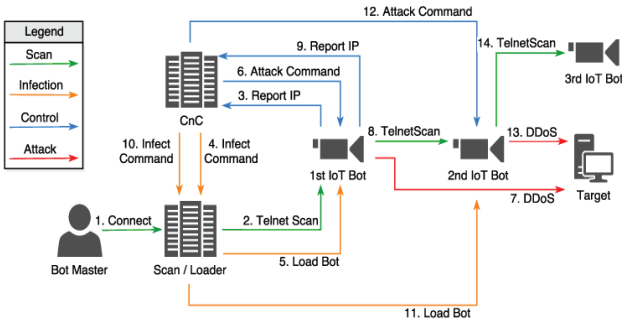

Fig.3 Mirai Botnet Infection Methodology

2. **XOR.DDoS**. XOR.DDoS appeared in 2015 and exploits the ShellShock vulnerability to infect devices. It can perform various types of DDoS attacks such as SYN Flood, UDP Flood, DNS Flood and TCP Flood.

The main features of XOR.DDoS:

- Compromise via ShellShock: exploiting a vulnerability to execute malicious code.
- High attack power: attacks reach millions of requests per second.

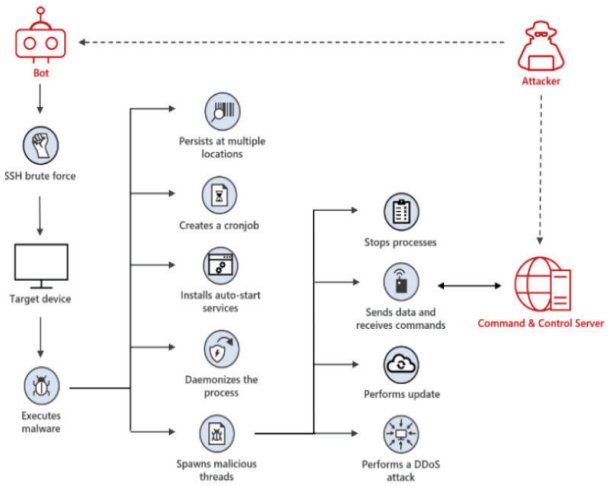

Fig.4 XOR.DDoS Infection Methodology

3. **Linux.Hydra**. Linux.Hydra appeared in 2008 and targets MIPS-based routers. It uses dictionary attacks or D-Link vulnerabilities to compromise. Once infected, the device becomes part of an IRC network and is capable of performing basic SYN Flood attacks.

Linux.Hydra features:

- Dictionary attack: brute force passwords to gain access.
- Exploitation of D-Link vulnerabilities: targeted attacks against specific routers.
- IRC integration: control via IRC channel.

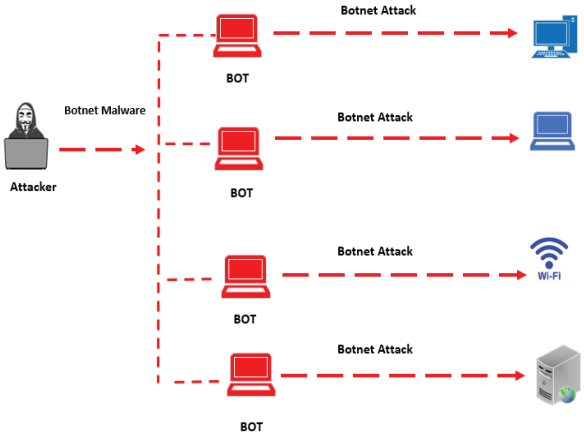

Fig.5 XOR.DDoS Infection Methodology

These three applications pose a serious threat to IoT networks, due to the possibility of using a large number of vulnerable devices to conduct massive DDoS attacks.

Recommendations for countering malicious DDoS software attacks

For Mirai:

- Strong passwords: set passwords that consist of a combination of upper and lower case letters, numbers, and special characters.
- Firmware updates: regularly update the firmware on IoT devices, including security updates.
- Traffic Filtering: configure traffic filters on network devices to detect and block abnormal or potentially malicious traffic.
- Port Closure: close TCP port 23 and disable the Telnet service on the router.

For XOR.DDoS:

- Changing passwords: change default passwords to strong passwords.
- Limit IP addresses: limit the number of IP addresses your IoT device connects to.

- Firewall: use a network firewall and DNS filtering to block potential SYN packets.
- Software Update: install software updates to address vulnerabilities.

For Linux.Hydra:

- Strong passwords: change default passwords to strong default passwords.
- Limit password attempts: configure the system to block password attempts after a certain number of failed attempts.

These measures can help reduce the risk of successful DDoS attacks on IoT networks, improving the overall security of your devices.

Conclusion

The paper elaborates on the key aspects of DDoS attacks, their patterns and process steps. It also focuses on three most popular viruses - Mirai, XOR.DDoS and Linux.Hydra - that are used to conduct such attacks. These viruses pose a serious threat to IoT networks as they can exploit vulnerabilities in these networks to conduct large-scale DDoS attacks. However, with proper knowledge and security measures, it is possible to counter these threats.

The paper also provides recommendations to counter these viruses, which include regular software updates, using strong passwords, limiting network access, and using specialized security tools. Given the rapid evolution of IoT technologies, it is important to continue research in this area to ensure the security and stability of IoT networks in the future.

Through such research, we can be better prepared to face potential threats and ensure that systems run smoothly.

References

1. Al-Hadhrami, Y., & Hussain, F. K. (2021). DDoS attacks in IoT networks: a comprehensive systematic literature review. World Wide Web, 24, 971–1001.
2. Kumar, P., Bagga, H., Netam, B. S., & Uduthalapally, V. (2022). SAD-IoT: Security Analysis of DDoS Attacks in IoT Networks. Wireless Personal Communications, 122, 87–108.
3. Kumar, P., Bagga, H., Netam, B. S., & Uduthalapally, V. (2021). DDoS Attack Detection Using Artificial Neural Network on IoT Devices in a Simulated Environment. In Advances in Computer Communication and Computational Sciences (pp. 221–230). Springer.
4. Study guide “The Internet of Things Technologies” [Online] - B.Yu. Zhurakovsky, I.A. Zenov – Retrieved from: https://ela.kpi.ua/bitstream/123456789/42078/1/Zhurakovsky i_B_Zeniv_Tehnologii_internet_rechey.pdf
5. Peng, T., Leckie, C., & Ramamohanarao, K. (2007). Survey of network-based defense mechanisms countering the DoS and DDoS problems. ACM Computing Surveys, 39(1), Article 3.
6. Granjal, J., Monteiro, E., & Sa Silva, J. (2015). Security for the internet of things: a survey of existing protocols and open research issues. IEEE Communications Surveys & Tutorials, 17(3), 1294–1312.
7. Kolias, C., Kambourakis, G., Stavrou, A., & Voas, J. (2017). DDoS in the IoT: mirai and other botnets. IEEE Computer, 50(7), 80–84.
8. Houle, K. J., & Weaver, G. M. (2001). Trends in denial of service attack technology. Tech. Rep., CERT Coordination Center, Pittsburgh, Pa, USA.
9. Bertino, E., Choo, K.-K. R., Georgakopolous, D., & Nepal, S. (2016). Internet of things (IoT): smart and secure service delivery. ACM Transactions on Internet Technology (TOIT), 16(4), Article 22.

Правило В.В., Аверкієв Є.О.

Аналіз шкідливого програмного забпезпечення з підтримкою DDoS-атак в мережах IoT

Проблематика. З поширенням мереж Інтернету речей (IoT) у цифрову епоху зростає і ризик кібератак, особливо DDoS-атак. IoT-пристрої, такі як розумні холодильники, термостати, веб-камери та інші побутові пристрої, підключені до Інтернету, стають мішенню для зловмисників, які можуть використовувати їх як частину ботнету для проведення DDoS-атак. Ці пристрої часто мають недостатній мережевий захист і рідко оновлюються, що робить їх уразливими. DDoS-атаки можуть призводити до значних збитків, таких як втрата доходу, шкода репутації та витрати на відновлення послуг. Отже, актуальною є проблема вразливості IoT-мереж до DDoS-атак та потреба в розробці ефективних заходів захисту.

Мета досліджень. Аналіз програмного забезпечення, що підтримує DDoS-атаки в мережах IoT. Надання загальних рекомендацій, які допоможуть покращити підходи до заходів захисту в мережах з технологією IoT, спрямованих проти шкідливого програмного забезпечення з підтримкою DDoS-атак.

Методика реалізації. Розглянуто п'ять основних моделей DDoS-атак: модель агент-обробник, рефлекторна модель, модель на основі IRC, веб-модель та модель на основі P2P. Проведено аналіз трьох найнебезпечніших програмних забезпечень, здатних здійснювати DDoS-атаки на IoT-мережі: Mirai, XOR.DDoS та Linux.Hydra.

Результати досліджень. Існує велика кількість моделей та методів здійснення DDoS-атак на IoT-мережі. Найбільш небезпечними є програмні забезпечення Mirai, XOR.DDoS та Linux.Hydra. Кожне з цих ПЗ має свої специфічні особливості та методи здійснення атак. Дослідження також показало, що існує декілька ефективних заходів для протидії цим атакам, включаючи встановлення сильних паролів, регулярне оновлення програмного забезпечення, налаштування фільтрів трафіку та обмеження доступу до мережі.

Висновки. Розглянуто ключові аспекти DDoS-атак, їх моделі та етапи процесу. Акцентовано увагу на трьох найнебезпечніших програмних забезпеченнях, які використовуються для проведення таких атак, та надаються рекомендації щодо протидії їм.

Ключові слова: *DDoS; IoT; кібератака; ботнет; шкідливе програмне забезпечення; Mirai; XOR.DDoS; Linux.Hydra; безпека мереж; протидія DDoS.*