# CNIT 37000

# A Comprehensive Study In The Distributed Denial Of Service (DDoS) Attack

Jiacheng Wang, Zach Gazda, Ian Zhao, Khay Qi Soo, Adnane Sentoussi

**Abstract**— Distributed denial of service (DDoS) attack is defined as a cyber-attack. This attack makes a machine or network resource temporarily unavailable to its intended users that are connected to the internet. Because DDoS attacks are simple, cheap, effective, and powerful to use, then lead to the DDoS attack becoming the most widely used cyber-attack right now. The primary objective of this report is to discuss how DDoS attack works and how to mitigate against it. The secondary objective of this report is to show how DDoS attacks use vulnerabilities to threaten a network. Also, two types of DDoS attack demonstrations will be introduced in this report as well.

## I. Introduction

During the Cyber-attack history, the DDoS attack is one of the oldest and the most dynamic attacks of cybercrime. The first known DDoS attack occurred all the way back in 1996 when an unknown attacker overwhelmed Panix, the oldest Internet Service Provider at the time, servers with an SYN Flood. This particular method took advantage of the TCP three-way handshake process by overriding a network with multiple fraudulent SYN packets coming from the fake IP address. Panix's servers ran out of resources and could no longer process requests from legitimate users, and it took them 36 hours to get back to normal.

### *A. What is DDoS Attack*

The primary goal of a DoS or DDoS attack is to make a network or machine resource unavailable to the intended users by either temporarily or permanently disrupting services of a host connected to the internet. These attacks are typically accomplished by overloading the targeted machine or network with an excess number of requests in an attempt to overload systems and prevent other user's requests from being fulfilled. The DDoS attack can forge the source IP address during the attack, which makes a perfect concealment of this attack when it happens. At the same time, it is exceedingly difficult to detect the attack. The traffic can mimic a legitimate GET request, which can make it exceedingly difficult to see the attack coming. It is especially important to always be prepared for DDoS attacks and the repercussions that could come with it[11].

The difference between the Dos and DDoS attack is that DDoS attacks have the incoming traffic originating from many different sources, making it impossible to put an end to the attacks by blocking one source. A layout of how the attack could go can be seen in Figure 1.

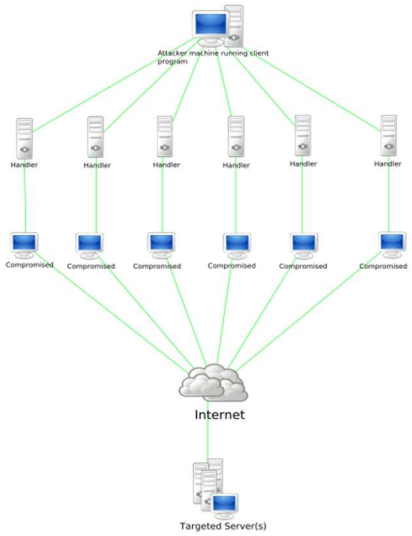



*Figure1: Diagram of a DDoS Attack*

### *B. Issues DDoS Attacks Can Create*

DDoS attacks can create a lot of issues for both users and business alike. First, it could cause a company's resources, like their website to be down for a while. Based on the severity of the attack, a company's website could be down for hours, days, or in a few cases, weeks. With the server being down for a period of time, it could start to affect a company's time and money. For time, the IT department could become more occupied with trying to get the servers back online, which could take away time from other responsibilities they may have. Regarding money, it could prevent users from being able to purchase products online or receive the help that they need with their technical issues.

### C. *DDoS Attack Today*

With the progress of the technology, this means that cyber network attacks are also constantly improving. The DDoS attacks also have developed into many different types and each type will focus on a specific target[1]. Today's DDoS attacks are commonly focused on layer 3(Network layer), layer 4(Transport layer) and layer 7(Application layer) [3]. And the layer 3 and layer 4 DDoS attacks are sending extremely high volumes of data to make the web server performance slow down, consume bandwidth and eventually the normal users could not access to the server. Therefore, these type of attacks are assigned into volumetric DDoS attacks on a network infrastructure, which could be called a volume-based attack. Layer 7 DDoS attack occupies the application processing resources of the server. It greatly consumes the processing performance of the server. These attacks are structured to overload the specific elements of an application's server infrastructure. Attacks aimed at this layer are called an Application layer attacks.

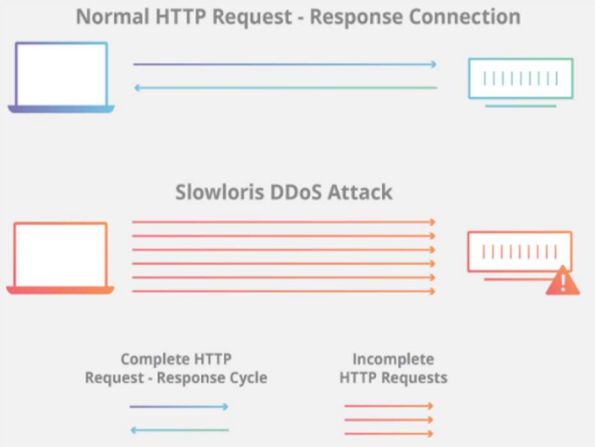
## II. RELATED WORK

### A. *Slowloris DDoS Attack*

Slowloris DDoS Attack is an application layer attack. This attack works by exploiting part of the HTTP request. The attacker first opens multiple connections to the target server by sending multiple partial HTTP request headers. The goal is open a thread for each incoming request, with the goal of closing the thread after the connection is complete. For efficiency, if the connection takes too long to finish, the server will timeout a very long connection, freeing the thread for the next request[9].

To prevent the target from timeout, the attack periodically sends part of the request header to the target to keep the request active. Essentially, the attack tells the server "I'm still here! I am very slow. Please wait for me." The target server can never release any open partial connections while waiting for the request to terminate. Once all available threads are used, the server will be unable to respond to additional requests from regular traffic, which results in a denial of service[12].

*Figure 2: Slowloris DDoS Attack*




### B. *SYN Flood Attack*

Every client-server conversation begins with a standardized three-way handshake. Thus, the attacker will send an overwhelming amount of SYN requests from the client to the server and the attacker will not responds to the server's ACK messages[8]. Then, the server will leave with open connections until further communication from the client. Because the server is open, many half-open connections occupy the server's connection table. This affects the normal users and the server to establish a session, then resulting in denial of services [11].

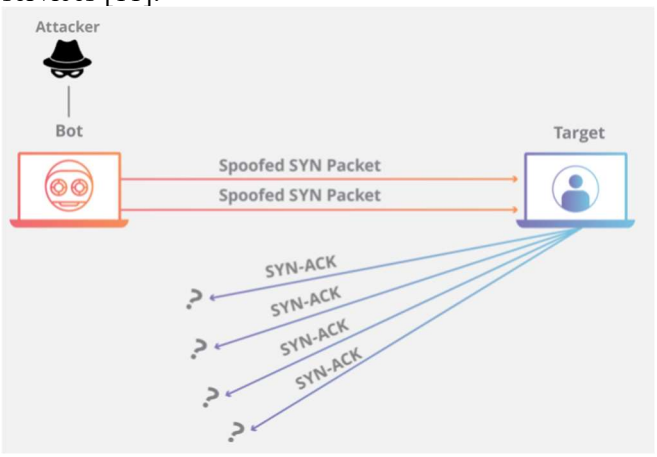



*Figure 3: SYN Flood Attack*

## III. EVALUATION

Under this section, we are going to show how we conducted the DDoS Attack demonstration, and before we start the experiment, we need set up the environment.

### A. *Project Design—Slowloris DDoS Attack*

In order to conduct the Slowloris DDoS Attack, we chose to use the pre-existing tools publicly available on the internet [5]. In the introduction section, we mentioned that today's DDoS attacks are mostly assigned into volume-based attack and Application layer attack. In the first demonstration we chose to do a Slowloris DDoS attack to attack a virtual machine target. This attack will determine what the vulnerabilities are.

The demonstration was carried out by using the following tools:

i. A Linux virtual machine with 4 CPUs and 8Gb RAM(Attacker)
ii. A Linux virtual machine with 4 CPUs and 8Gb RAM(Target)
iii. Wireshark
iv. Slowloris software installation

#### a. *Environment Setup*

Before we start to test the Slowloris DDoS attack, we created a website use on the target server virtual machine to show how the Slowloris DDoS attack could impact the network (See Figure 4).

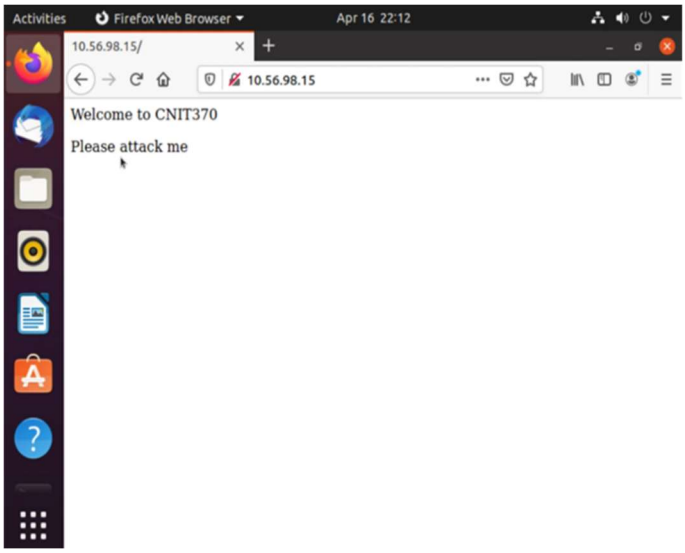



*Figure 4: Target website*

### b. Conducting the Attack

After we set up the website and the IP address for each virtual machine, we then installed the Slowloris software from the internet. We then readied the Slowloris python script with the IP address of the target virtual machine, we used the command *python slowloris-py 10.56.98.15.*

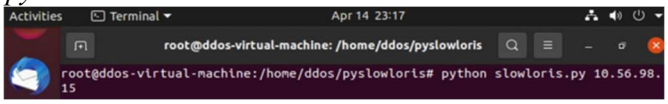



*Figure 5: Slowloris DDoS attack command*

Before we execute the Slowloris python script, we opened the Wireshark software on the target virtual machine to monitor packets that are sent by the attacker's virtual machine. As the script is executed, the Wireshark cached the packet immediately. We were able to see the packet was send to the IP address 10.56.98.15 and it is from the IP address 10.56.98.20, and the packet is sent by TCP protocol(See Figure 5).

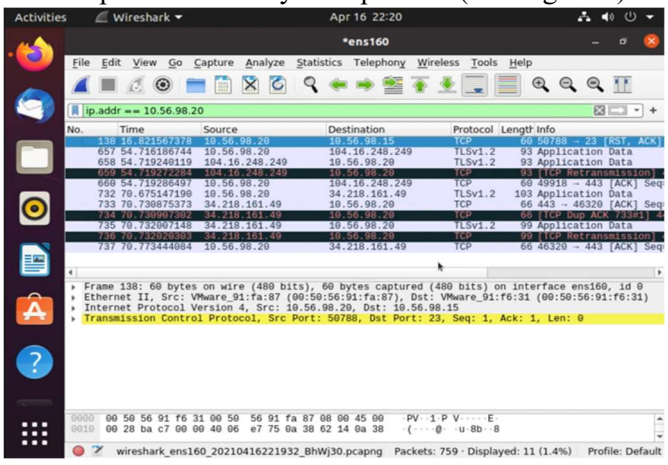



*Figure 5: Wireshark capture*

## B. Project Design —SYN Flood Attack

In order to conduct the SYN Flood Attack, we chose to use the hping3 software from the internet resources.[6]

The demonstration was carried out by using the following tools:

i. A Linux virtual machine with 4 CPUs and 8Gb RAM(Attacker)
ii. A Linux virtual machine with 4 CPUs and 8Gb RAM(Target)
iii. Setting up a website
iv. Hping3 software installation

The two virtual machines are already created by previous Slowloris DDoS attack demonstration, we only need to download and install the hping3 software into the attacker virtual machine and run it. So, the hping3 is a network tool that able to send the custom TCP/IP packets and could also display the target's replies.

The best way method for this attack is to use a Windows 10 system virtual machine as the target, but due to the limitations of resources, we used a Linux virtual machine as the target.

### a) Environment Setup

For this demonstration, the environment was set up by using two Linux virtual machines. We used the command *sudo apt-get install -y hping3* to install the hping3 software. After the hping3 software finished installing, we opened Wireshark on the target virtual machine and ready to capture the TCP/IP packet that sent by the attacker. [7]

Before we execute the hping3 command, we used the command *sudo apt-get update* and *sudo apt-get upgrade* to make sure the virtual machine is updated and upgraded.

### b) Conducting the Attack

Before we execute the hping3 attack command, we opened the website that we created for the target and opened the Wireshark on the target virtual machine as well.

Then we executed the command on the attacker virtual machine, the command used as following:

*sudo hping3 10.56.98.15 -p 23 -s 50788 -R -A -M 218417699 -L 2052727860 -c 1*

- 10.56.98.15 is the IP address of the victim.
- 23 is the port number.
- 50778 is the source port.
- 218417699 is the TCP seq number.
- 2052727860 is the TCP ack number and 1 means send only one packet.

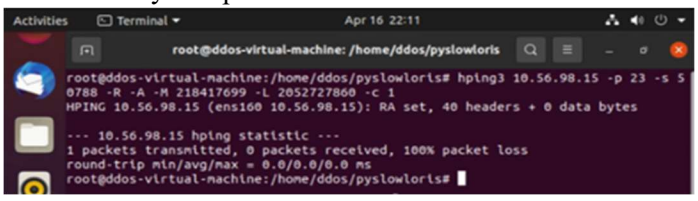


*Figure 6: hping3 attack command*

After the hping 3 attack command was executed, Wireshark captured the packet that sent by the attack.

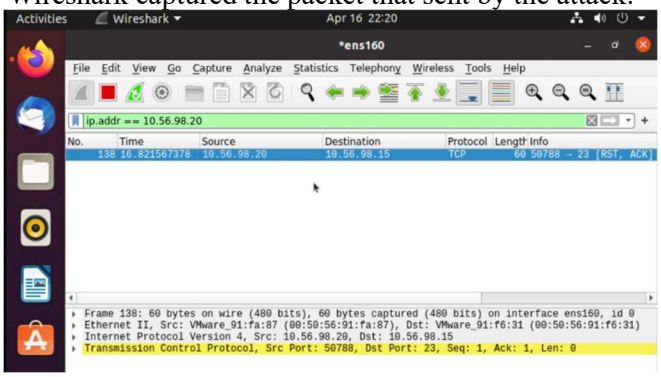



*Figure 7: hping3 attack Wireshark capture*

## IV. VULNERABILITY EXPLANATION

### *A. Cheap Hosting*

The first vulnerability that leads to DDoS attacks would be using cheap hosting. Cheap hosting has two main downsides, which include the low machine volume and lack of support. The DDoS attack mainly uses excessive traffic to overwhelm the server, which makes the server unable to respond to regular traffic. The limited machine volume means the attacker can easily pass the allowed bandwidth provided by the server. With the cheap hosting, many clients might share the same server, which means one site that gets attacked will affect the other sites that not on the attacker's list.

The cheap hosting also has a problem at providing support, and the provider will not be able to provide DDoS attack security precautions. The limited budget will not allow the provider to regularly backup the code and help repair or restore the server. The provider might not even be able to provide a warning when the DDoS attack is taking place.

### *B. Lack of Preparation*

Lack of preparation for the possible DDoS attack will aggravate the loss since there is no backup or safety precaution regarding the attack. Taking safety precautions like installing security software will enhance staying online even if the attack is taking place. The security software will alert the owner when it notices the server is under the DDoS attack, and the owner can take action like IP filtering to protect the server. The preparation can also help the owner recover the server more quickly when the site went down. Regular backup of the data can help restore the data and make the server go up as soon as possible.

### *C. Insecure or Out of Date Code*

Out-of-date code and insecure code will not make the server vulnerable to the DDoS attack. However, this does not mean that it will not have other bad influences. When the server gets overwhelmed by the DDoS attack, the attacker will have the chance to gain access to the server. The out-of-date or insecure code will make getting access much easier for the attacker since they already know the existing bugs. Once the attacker gets unwanted access, they might leak the user data and other vital data. Keeping the code up to date and using the plugin from reputable sources will help the owner mitigate loss when subjected to an attack.

## V. MITIGATION

### *A. Four Stages of Mitigation*

The first stage that is involved in mitigating a DDoS attack is detection. A website needs to be capable of identifying an attack from a normal or heavy traffic. Collecting data on common attack patterns, IP reputation, and previous data will be helpful in proper detection. If an attack is detected, the website needs to be able to stop attackers that disguised as legitimate visitors from viewing the content of the webpage to minimize the damage caused.

The next stage to stop a distributed attack is response. A good DDoS protection network needs to be able to drop and reject malicious bot traffic that is incoming from an identified threat and absorb the rest of the traffic without affecting normal users from using or browsing the website. This can be done by configuring a Web Application Firewall to mitigate application layer attacks and handling attacks on the network and transport layer by applying another filtration process such as another firewall.

The third stage that is involved in the mitigation of a DDoS attack is routing. By applying an effective routing solution, incoming traffic will be broken down into smaller, manageable chunks in order to prevent DDoS attacks. [2]

The last stage of mitigation is adaptation. A good protection service needs to be able to harden itself against future attacks by analyzing past traffic for patterns like improper protocols being used, repeated offending IP blocks, and attack patterns originated from certain countries. [10]

### *B. Important Characteristics of a DDoS Mitigation Service*

Scalability is one of the must-have characteristics of a DDoS mitigation service. An effective DDoS protection network needs to have the capability of adapting to the growing needs of an expanding business and handle the increasing scope of DDoS attacks.

Secondly, flexibility is also an important characteristic to factor in when choosing a DDoS mitigation service. It is important to be able to add policies when needed to a web service to adapt to real-time threats.

Being able to implement additional rules and applying changes immediately across the whole network is also critical in keeping a site live when attack occurs.

Next, reliability is an important feature that a DDoS mitigation service should provide. The success of protection strategies implemented relies heavily on the reliability of a DDoS solution. The mitigation service should also be able to provide redundancy and support fail-over of the data centers. The service needs to have high uptime rates and be able to identify new threats 24 hours a day.

Lastly, the network size is also a critical attribute of a DDoS protection network. The attack vectors and patterns of DDoS attacks that occur across the Internet change over time. Therefore, having a large network with great bandwidth allows DDoS mitigation services to quickly analyze and respond to attacks in an efficient manner. Attacks could be stopped before they ever occur if they are being handled in a timely manner.

## VI. Discussion and Future Work

### A. DDoS usage today

DDoS attacks are still very alive and well today. There were 10 million DDoS attacks in 2020 alone. One reason for the increase in DDoS attacks in 2020 was cybercriminals taking advantage of the increase usage of the internet because of the COVID-19 pandemic. With a lot of people having to work remotely from home, cyber-criminals would do anything they could do bring a network offline and offer to bring it back up in exchange for money. The size of the attacks also increased in 2020, as Amazon Web Services reported mitigating a 2.3 Tbps attack. There is expected to be an even greater increase in DDoS attacks in years to come according to Figure 8 below.

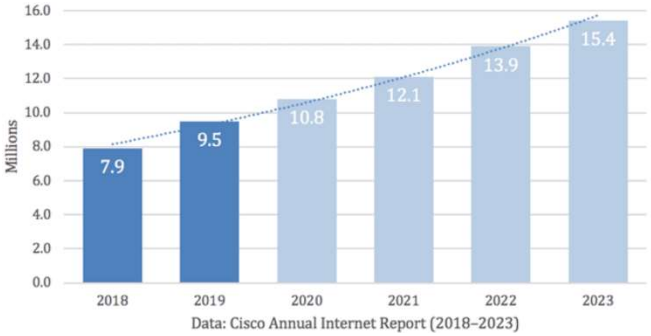



*Figure 8: Estimate for DDoS attacks that will occur in years to come.*

### B. Instance of a DDoS attack

It is important to note that even some of the biggest companies are prone to having their servers go down if a DDoS attack is successful. Back in October of 2016, Dyn [13], a major DNS provider at the time, was hit with a nasty 1.3 Tbps DDoS attack. A group of hackers created a massive Mirai botnet that incorporated IoT devices to launch the largest DDoS attack at the time. Because Dyn was a DNS provider for companies like Amazon, Netflix, PayPal, and others, it caused a lot of their client's websites to not function properly. Dyn was able to mitigate the attacks within a few hours, but the attack also had nasty trickle-down effects and caused some sites that relied on Dyn to be down for a slightly longer period. To this day, this DDoS attack is still one of the most impactful attacks ever, as it managed to bring down a good amount of America's internet in a short amount of time.

### C. Regulations regarding DDoS

DDoS attacks are illegal under the Computer Fraud and Abuse Act of 1986. It could land a perpetrator up to 10 years in prison as well as a fine up to $500,000. The only problem is that the law does not stop malicious hackers from performing DDoS attacks on enterprises. To combat this, companies are trying to invest more into DDoS mitigation services to help reduce the repercussions that come with a DDoS attack. The FBI and the Cybersecurity and Infrastructure Security Agency are currently in charge of conducting cyber forensics to see when and where the DDoS attacks were conducted. Unfortunately, with the attacks being DDoS, they are very hard to track because due to multiple botnets being implemented for an attack. It is wise to be cautious of what is being downloaded because there is a chance that it could contain malware that could be used against the downloader.

### D. Future Work

For understanding mitigation and how attacks are developed, we need to have a clear understanding of what will happen during the attack. For that, a DDoS attack can be achieved by exploiting a vulnerability on the server, or by consuming resources on the server (such as memory, hard disk, and so on.).

To mitigate DDoS attacks, we could optimize resource usage to improve the load capacity of the Web Server, also use highly scalable DNS devices to protect DDoS attacks against DNS. By enable anti-IP spoofing on the router or firewall could also help to mitigation the DDoS attack from the IP spoofing.

## VII. Conclusion

DDoS attacks are one of the most complex attacks in cybercrime and cause losses in both time and money for an enterprise. With DDoS attacks projected to increase year-by-year, it is important to have the right mitigation services in place to prevent the collateral damage that DDoS attacks can cause. It is also important for users to be wary about what they download from an email or the internet, as they could contain malware that could be used against them in the future. By educating users and with the right mitigation and by approaching

things with a degree of caution, DDoS attacks can be stopped in terms of the damage they can do.

## VIII. REFERENCES


[1] 25, F., 18, F., 25, J., & 11, J. (2021, March 24). *Layer Seven DDoS Attacks*. Infosec Resources. https://resources.infosecinstitute.com/topic/layer-seven-ddos-attacks/#:~:text=They%20attack%20the%20top%20layer%20OSI%20model.

[2] Cloudflare. (n.d.). *What is DDoS Mitigation?* Cloudflare. https://www.cloudflare.com/learning/ddos/ddos-mitigation/.

[3] DDoS QUICK GUIDE. (2020, October). https://us-cert.cisa.gov/sites/default/files/publications/DDoS%20Quick%20Guide.pdf.

[4] Elvin, Tobi N., Laxmana P., & camp0. (2018, August). Hping3 doesn't work? Information Security Stack Exchange. https://security.stackexchange.com/questions/185048/hping3-doesnt-work.

[5] Gkbrk. (n.d.). *gkbrk/slowloris*. GitHub. https://github.com/gkbrk/slowloris.

[6] hping3(8) - Linux man page. (n.d.). https://linux.die.net/man/8/hping3#:~:text=Description,files%20encapsulated%20under%20supported%20protocols.

[7] *hping3*. Penetration Testing Tools. (n.d.). https://tools.kali.org/information-gathering/hping3.

[8] Imperva. (2020, September 30). *What is a TCP SYN Flood: DDoS Attack Glossary: Imperva*. Learning Center. https://www.imperva.com/learn/ddos/syn-flood/.

[9] Imperva. (2020, September 30). *What is Slowloris?: DDoS Tools: Imperva*. Learning Center. https://www.imperva.com/learn/ddos/slowloris/.

[10] *What Is a DDoS Attack and How to Stay Safe from Malicious Traffic Schemes: McAfee Blogs What is a DDoS attack and how does it work?: McAfee Blog*. McAfee Blogs. (2021, March 26). https://www.mcafee.com/blogs/consumer/consumer-threat-notices/ddos-attack-work/.

[11] What is a DDoS Attack? (2020). https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/.

[12] *What is a Slowloris DDoS Attack?* NETSCOUT. (n.d.). https://www.netscout.com/what-is-ddos/slowloris-attacks.

[13] Woolf, N. (2017, May 15). *DDoS attack that disrupted internet was largest of its kind in history, experts say*. The Guardian. https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet