RouterOS, Firewall, and Beyond: Maintain IP Reputation Over the Internet

By Michael Takeuchi

20 October 2018, Yogyakarta

MikroTik User Meeting Indonesia 2018

Little Things About Me

- Was MikroTik Certified on MTCNA, MTCRE, MTCINE, MTCUME, MTCWE, MTCTCE, MTCIPv6E, Consultant
- 3 July 2017 – 22 September 2018
  Work as Network Analyst at
  PT. Maxindo Mitra Solusi
- Studies at Bina Nusantara University

https://www.linkedin.com/in/michael-takeuchi
https://www.facebook.com/mict404
michael@takeuchi.id

Maxindo?
maxindo.net.id

- Maxindo or Maxindo Mitra Solusi, PT is One of Internet Service Provider (ISP) in Indonesia with Coverage in Jakarta, Bogor, Depok, Tangerang, Bekasi, Rangkas Bitung, Serang, Cibinong, Cikarang, Surabaya, Malang & Bali
- Not Only Internet Service Provider, Maxindo Also Provide "*Business Support*" that will help your business with our provided solution (Hosting, Virtual Private Network or VPN, WiFi & Hotspot, Consultation, Audit, Optimization etc.)
- One of our customer care, we always monitor any **malicious or anomalies traffic** on entire Maxindo Network (Powered by MikroTik as IDS & Honeypot ☺) and notify our customer if there is a malicious or anomalies traffic
- Me, The one of ~~*Satpam*~~ ***Security*** in Maxindo ☺

Presentation Outline

- What is Reputation
- Reputation in Computer Networking
- Reputation Check
  - Online Reputation Checker
  - How it works?
  - Blacklist Database
- Root Cause Analysis of Bad Reputation
- Impact of Bad Reputation
- Mitigation of Bad Reputation
- Conclusion

Reputation?

What is Reputation?

- **Reputation** or **image** of a social entity (a person, a social group, or an organization) is an opinion about that entity, typically as a result of social evaluation on a set of criteria.

  - Wikipedia,

  https://en.wikipedia.org/wiki/Reputation

Reputation in Computer Networking?

- Reputation that we know is an opinion about that entity, typically as a result of social evaluation on a set of criteria. And this one also applicable on Computer Networking
- If we see reputation by person, in Computer Networking we see reputation by IP Address

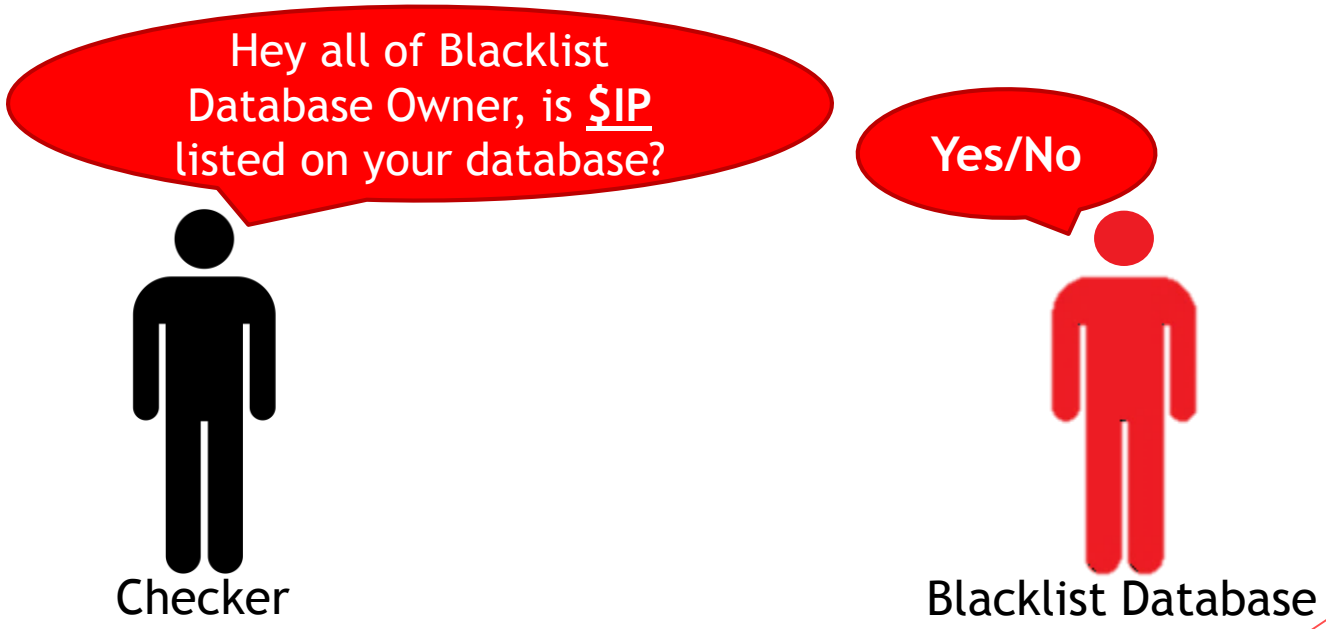
Reputation Check (Online Reputation Checker)

- https://bgp.he.net
- https://mxtoolbox.com/blacklists.aspx
- https://www.dnsbl.info

etc.

Reputation Check (How it works?)

How it works?



Reputation Check (Blacklist Database)

IP Info | Whois | DNS | RBL

Failed 0 out of 105 tests.

access.redhawk.org	PASS
all.spamblock.unit.liu.se	PASS
b.barracudacentral.org	PASS
bl.deadbeef.com	PASS
bl.emailbasura.org	PASS
bl.spamcannibal.org	PASS
bl.spamcop.net	PASS
blackholes.five-ten-sg.com	PASS
blackholes.mail-abuse.org	PASS
blacklist.sci.kun.nl	PASS
blacklist.woody.ch	PASS
bogons.cymru.com	PASS
bsb.spamlookup.net	PASS
cbl.abuseat.org	PASS
cbl.anti-spam.org.cn	PASS
cblless.anti-spam.org.cn	PASS
cblplus.anti-spam.org.cn	PASS
cdl.anti-spam.org.cn	PASS
combined.njabl.org	PASS

This is only few of many Blacklist Database from bgp.het.net online reputation checker

Root Cause Analysis of Bad Reputation

Root Cause of Bad Reputation

- Malicious/Anomalies Traffic
  - Botnet
  - Flooding
  - Spamming
  - Denial of Services/Distributed Denial of Services
- Bruteforce Login
- Copyright Infringement

etc.

Malicious/Anomalies Traffic

- Some packets that has been sent abnormally and may be harm a system or services on the internet or on your Local Area Network
- Usually generated by *botnet* from the *infected devices*
- You can torch and see all of your network traffic

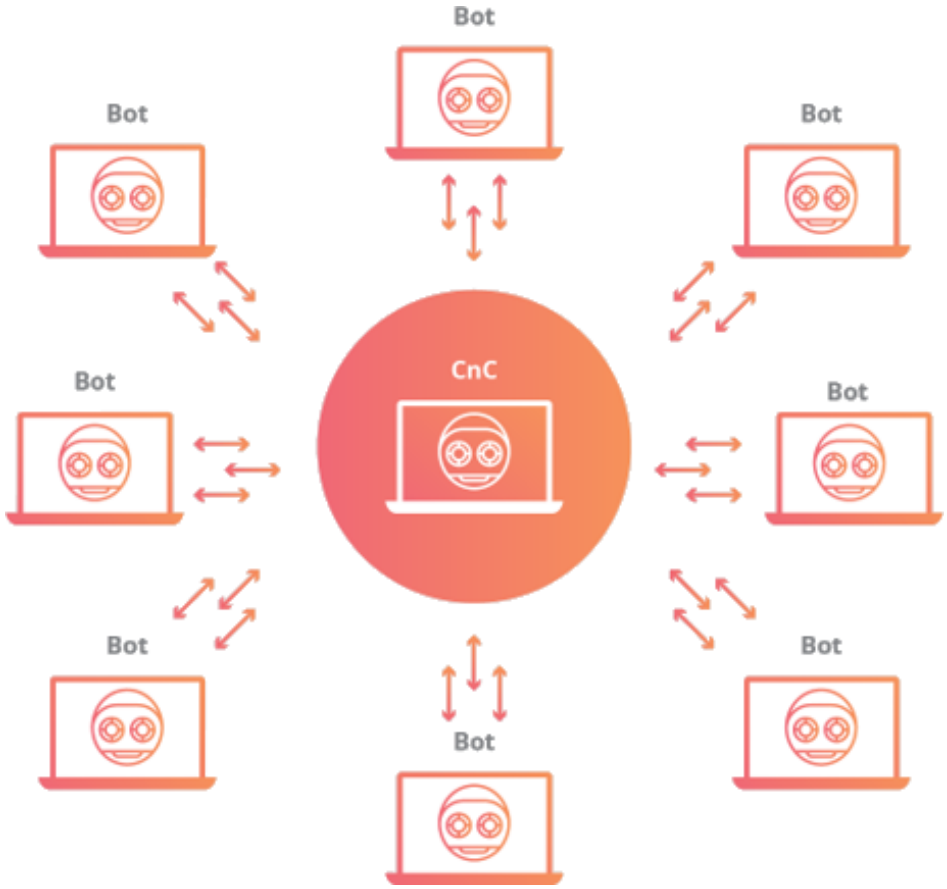
Botnet

- A botnet is a number of Internet-connected devices, each of which is running one or more bots. Botnets can be used to perform **distributed denial-of-service attack (DDoS attack)**, steal data, **send spam**, and allows the attacker to access the device and its connection. The owner can control the botnet using command and control (C&C) software. The word "botnet" is a combination of the words "robot" and "network". The term is usually used with a negative or **malicious** connotation.

- Wikipedia

https://en.wikipedia.org/wiki/Botnet

Botnet



https://www.cloudflare.com/learning/ddos/what-is-a-ddos-botnet/

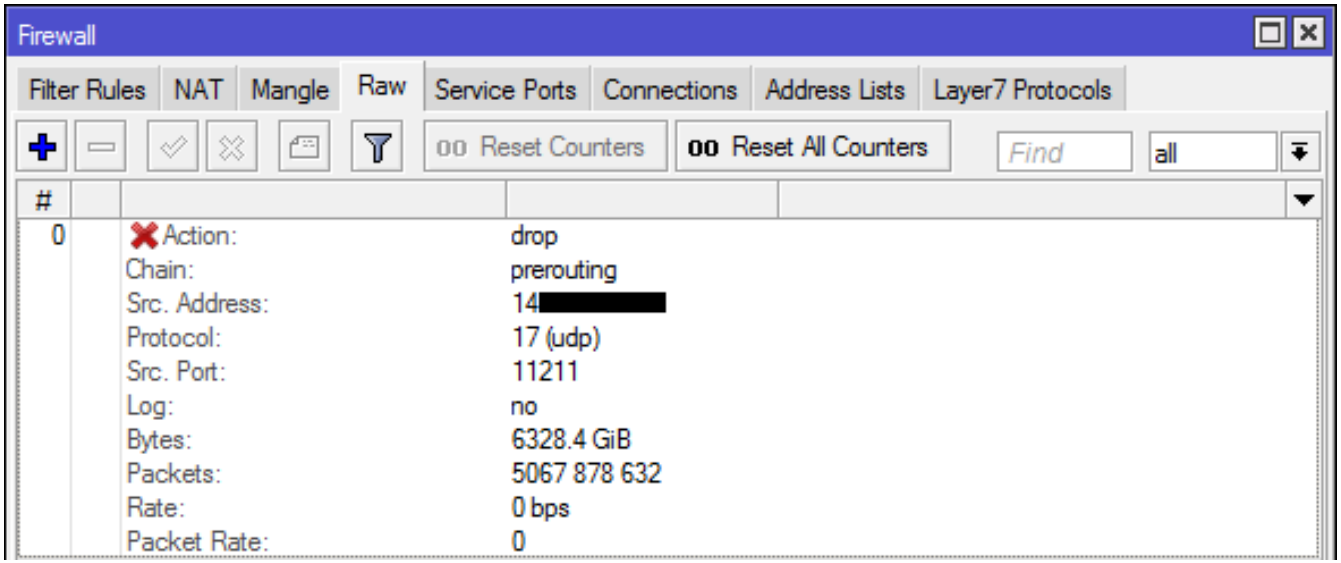
Flooding

- Imagine when 1 Little House got 1000 Guest
- In computer networking let's say, you have a router and your internet bandwidth capacity is 10Mbps but you got attack and make your link capacity is full

Request > Capacity

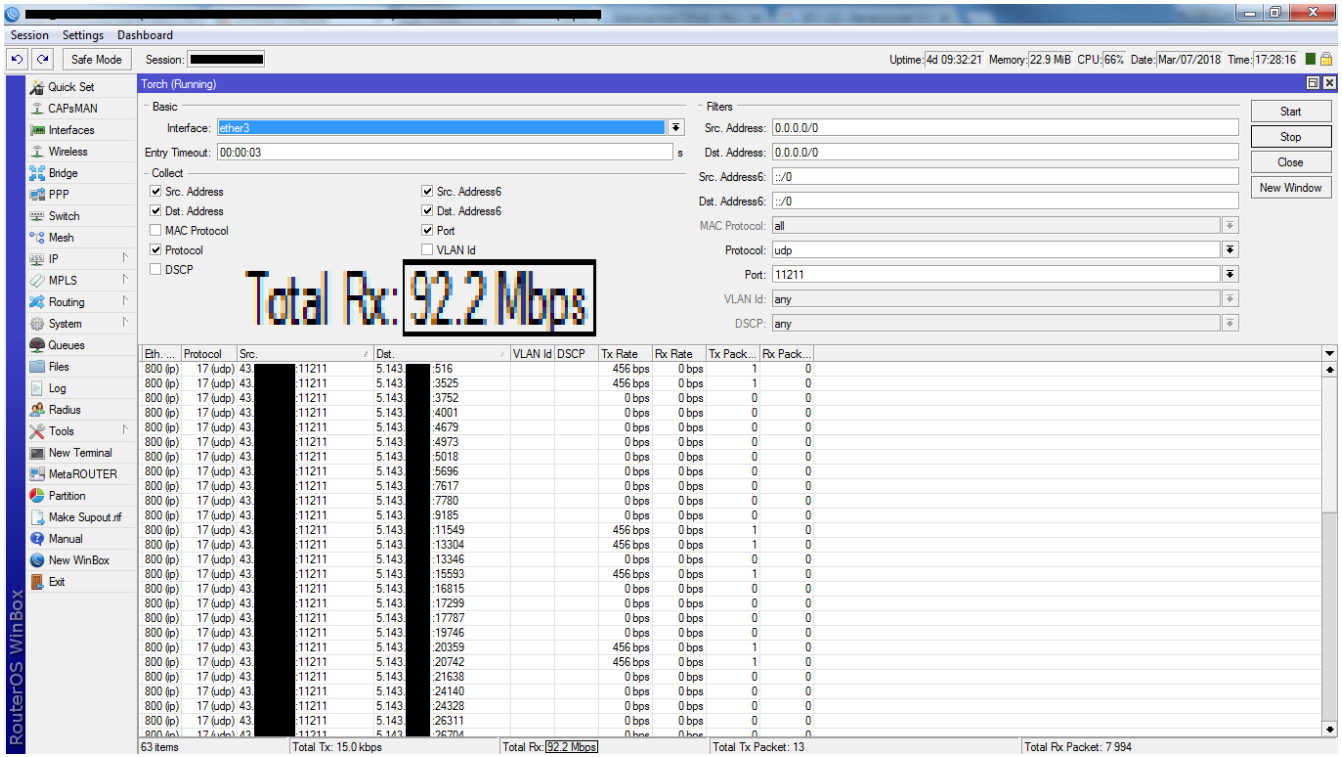
(more than)

Flooding Example

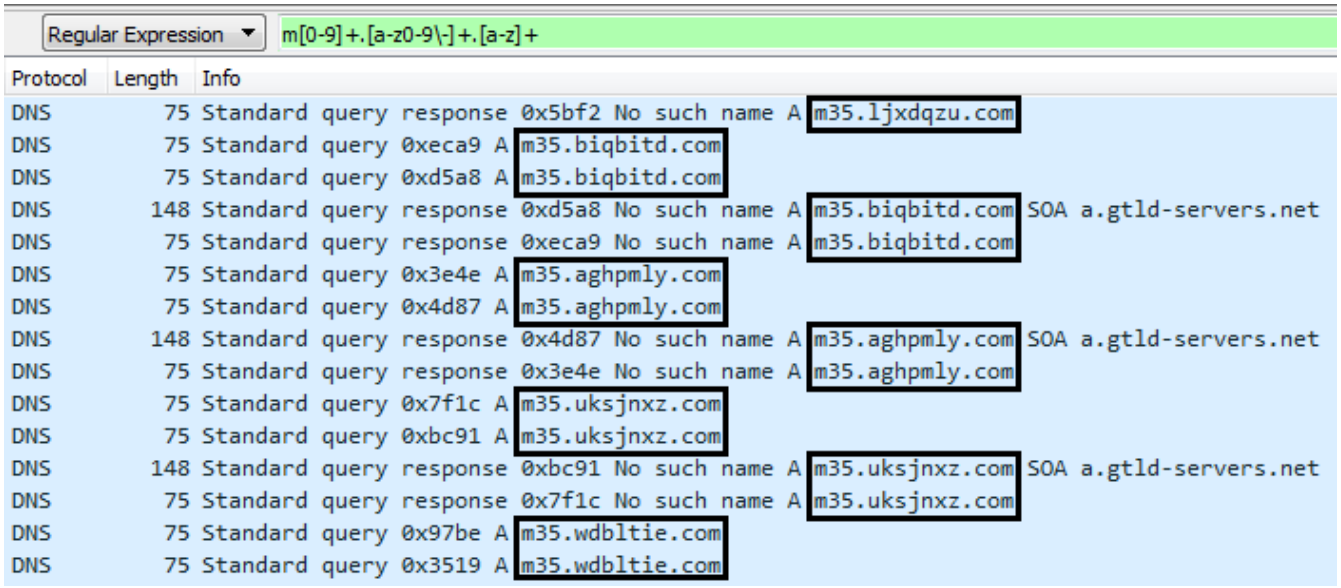


We have 6328.4GB with 5.067.878.632 Packets from UDP/11211 the flood was make the link full and got intermittent

Flooding Example



Flooding Example

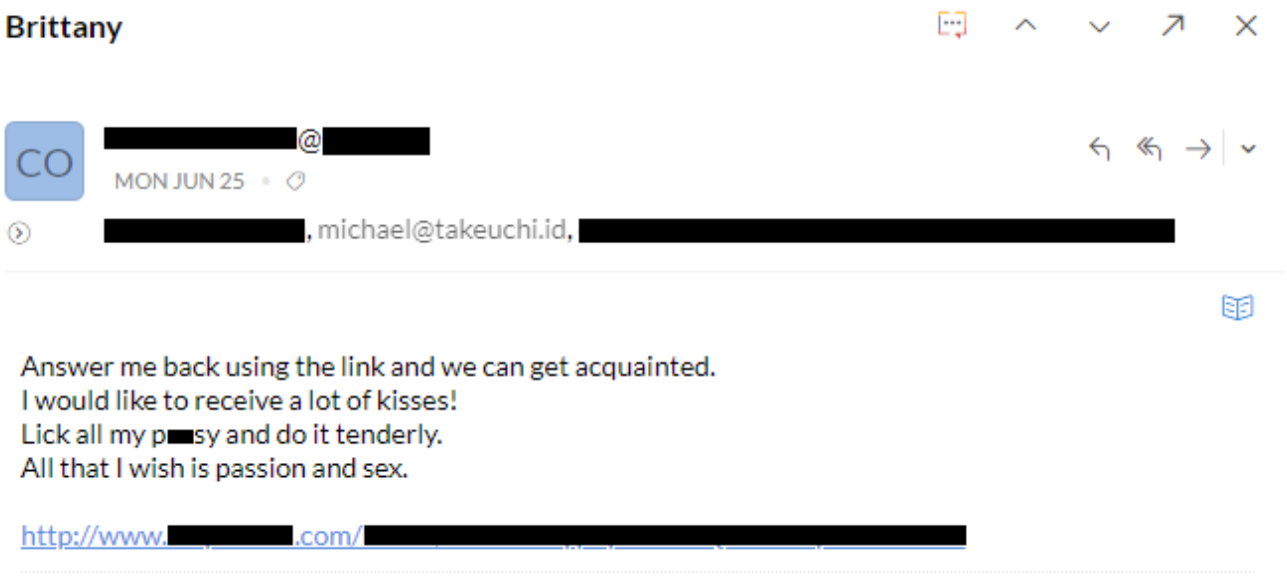


Regular Expression: m[0-9]+.[a-z0-9\-]+.[a-z]+

Protocol	Length	Info
DNS	75	Standard query response 0x5bf2 No such name A m35.ljxdqzu.com
DNS	75	Standard query 0xeca9 A m35.biqbitd.com
DNS	75	Standard query 0xd5a8 A m35.biqbitd.com
DNS	148	Standard query response 0xd5a8 No such name A m35.biqbitd.com SOA a.gtld-servers.net
DNS	75	Standard query response 0xeca9 No such name A m35.biqbitd.com
DNS	75	Standard query 0x3e4e A m35.aghpmly.com
DNS	75	Standard query 0x4d87 A m35.aghpmly.com
DNS	148	Standard query response 0x4d87 No such name A m35.aghpmly.com SOA a.gtld-servers.net
DNS	75	Standard query response 0x3e4e No such name A m35.aghpmly.com
DNS	75	Standard query 0x7f1c A m35.uksjnxz.com
DNS	75	Standard query 0xbc91 A m35.uksjnxz.com
DNS	148	Standard query response 0xbc91 No such name A m35.uksjnxz.com SOA a.gtld-servers.net
DNS	75	Standard query response 0x7f1c No such name A m35.uksjnxz.com
DNS	75	Standard query 0x97be A m35.wdbltie.com
DNS	75	Standard query 0x3519 A m35.wdbltie.com

Spamming

Spamming



Brittany

CO [redacted]@[redacted]

MON JUN 25

[redacted], michael@takeuchi.id, [redacted]

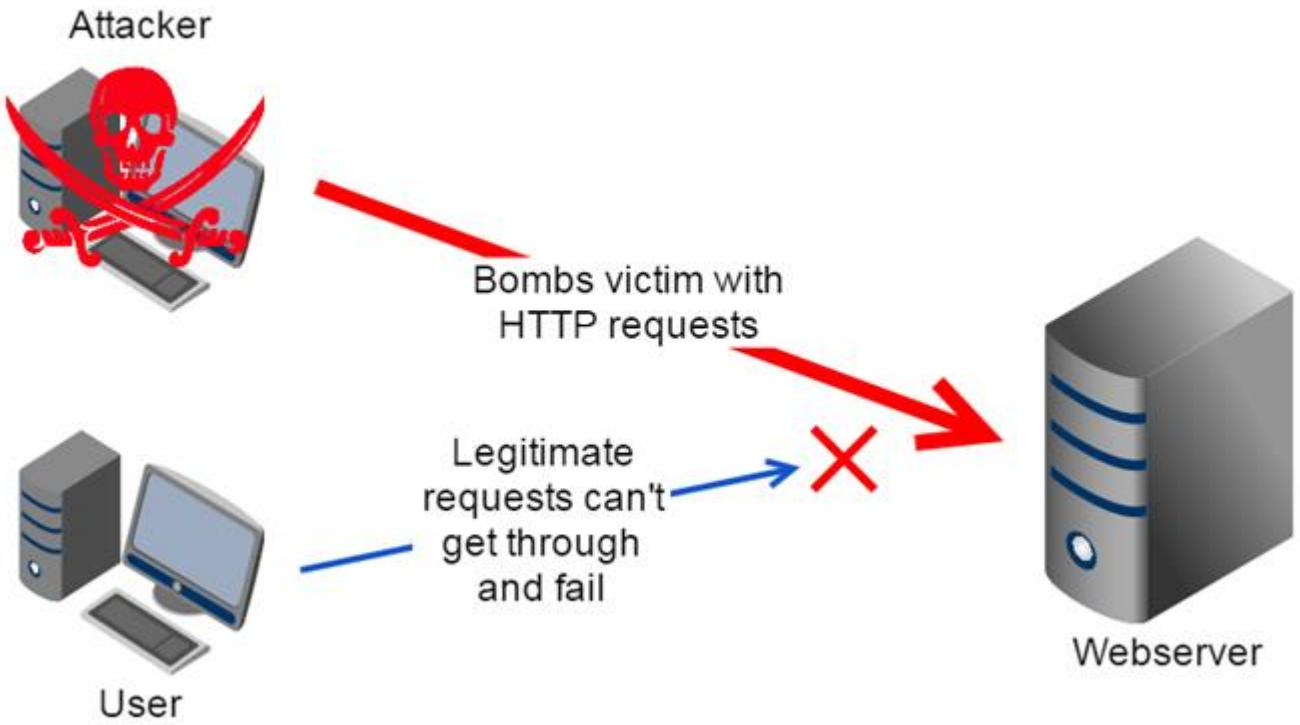
Answer me back using the link and we can get acquainted.
I would like to receive a lot of kisses!
Lick all my p[redacted]sy and do it tenderly.
All that I wish is passion and sex.

http://www.[redacted].com/[redacted]

Denial of Services *&* Distributed Denial of Services

- Kind of Flooding and make a "*services*" DOWN
- Imagine when 1 little house serve 1000 Guest can it happen? **Of course NO!** The house will overload and can't serve as usual

Denial of Services & Distributed Denial of Services



Images was taken from about31.net

Denial of Services *VS* Distributed Denial of Services

- DOS attacks are simultaneously launched from one sources destinated to the same target
- DDoS attacks are simultaneously launched from several sources destinated to the same target

DOS	DDoS
One Attacker to One Target	Many Attacker to One Target

Bruteforce Login

Log

Freeze

Apr/10/2018 16:58:27	memory	system, error, critical	login failure for user user from 72.230.199.192 via telnet
Apr/10/2018 16:58:31	memory	system, error, critical	login failure for user root from 72.230.199.192 via telnet
Apr/10/2018 16:58:33	memory	system, error, critical	login failure for user root from 72.230.199.192 via telnet
Apr/10/2018 16:58:34	memory	system, error, critical	login failure for user root from 72.230.199.192 via telnet
Apr/10/2018 16:58:38	memory	system, error, critical	login failure for user root from 72.230.199.192 via telnet
Apr/10/2018 16:58:40	memory	system, error, critical	login failure for user root from 72.230.199.192 via telnet
Apr/10/2018 16:58:42	memory	system, error, critical	login failure for user root from 72.230.199.192 via telnet
Apr/10/2018 16:58:45	memory	system, error, critical	login failure for user guest from 72.230.199.192 via telnet
Apr/10/2018 16:58:47	memory	system, error, critical	login failure for user service from 72.230.199.192 via telnet
Apr/10/2018 16:58:48	memory	system, error, critical	login failure for user root from 72.230.199.192 via telnet
Apr/10/2018 16:58:52	memory	system, error, critical	login failure for user supervisor from 72.230.199.192 via telnet
Apr/10/2018 16:58:53	memory	system, error, critical	login failure for user root from 72.230.199.192 via telnet
Apr/10/2018 16:58:55	memory	system, error, critical	login failure for user root from 72.230.199.192 via telnet
Apr/10/2018 16:59:00	memory	system, error, critical	login failure for user root from 72.230.199.192 via telnet
Apr/10/2018 16:59:01	memory	system, error, critical	login failure for user root from 72.230.199.192 via telnet
Apr/10/2018 16:59:03	memory	system, error, critical	login failure for user admin from 72.230.199.192 via telnet
Apr/10/2018 16:59:06	memory	system, error, critical	login failure for user root from 72.230.199.192 via telnet
Apr/10/2018 16:59:08	memory	system, error, critical	login failure for user guest from 72.230.199.192 via telnet

Piration

Notice of Claimed Infringement - Case ID [redacted]

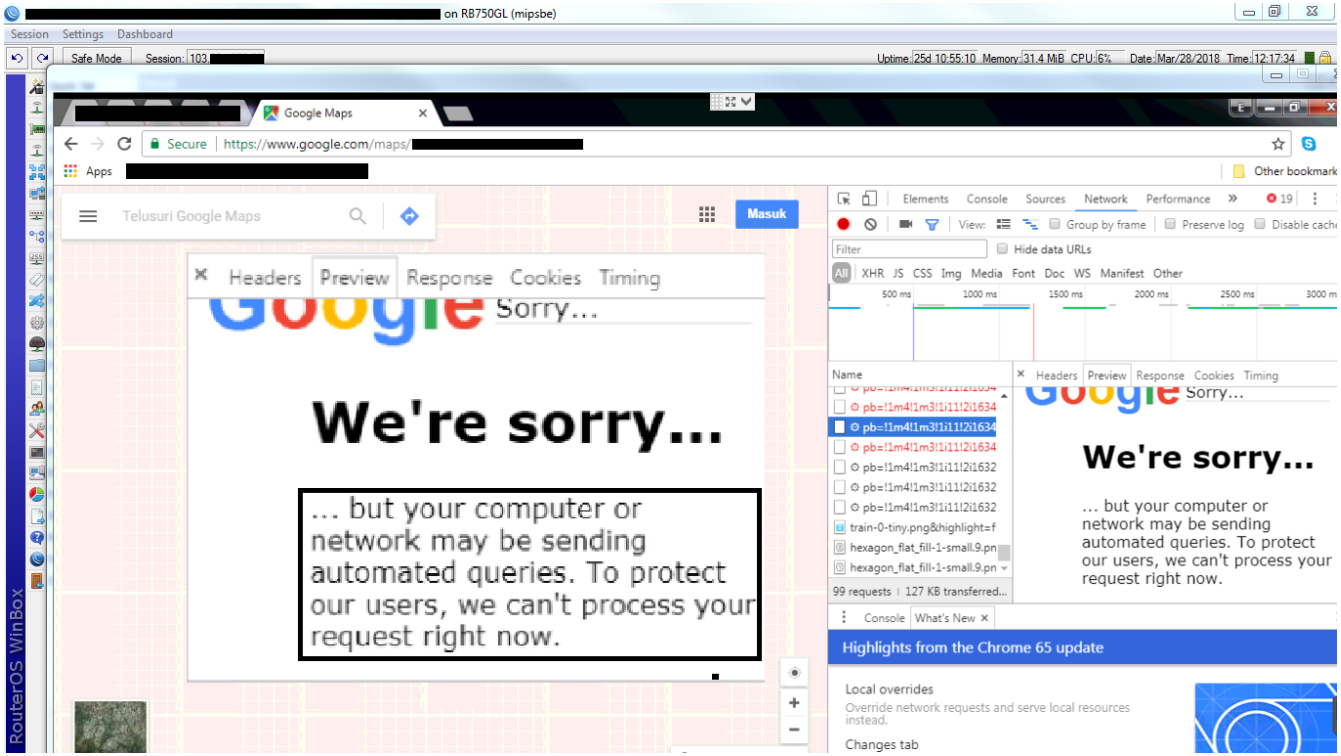
Evidentiary Information:
Protocol: BITTORRENT
Infringed Work: Transformers: The Last Knight
Infringing FileName: Transformers.The.Last.Knight.2017.1080p.WEB-DL.DD5.1.H264-FGT
Infringing FileSize: 6377875658
Infringer's IP Address: 175.[redacted]
Infringer's Port: 1798
Initial Infringement Timestamp: 2018-04-11T23:33:43Z

Impact of Bad Reputation

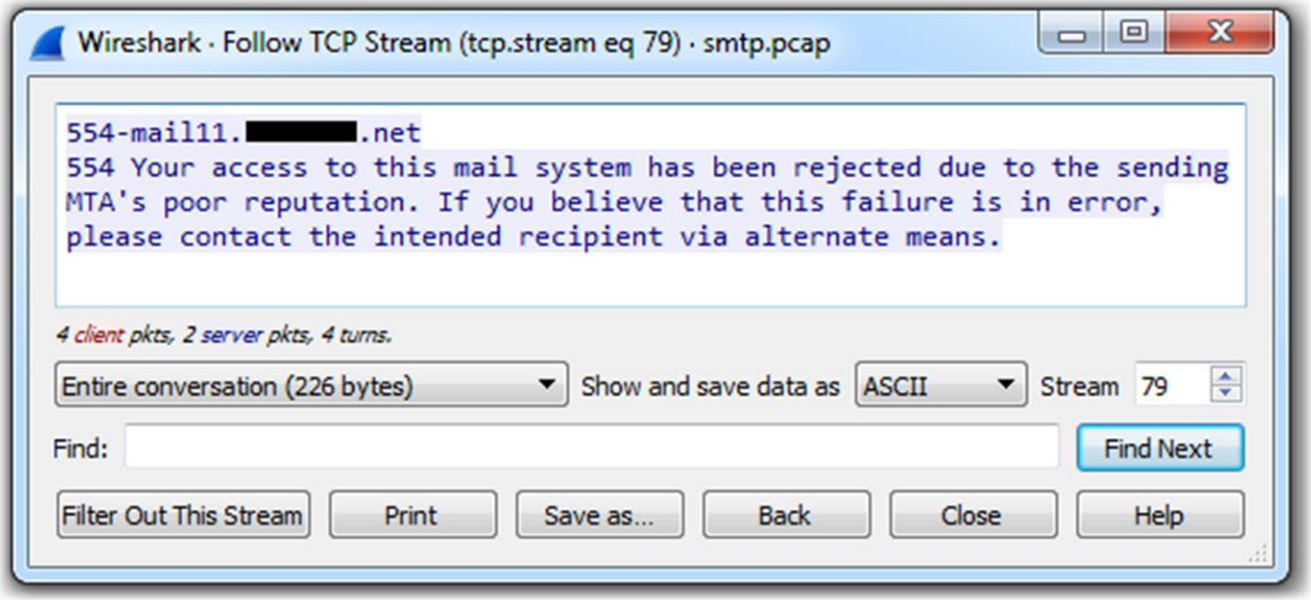
Impact of Bad Reputation

- Blacklisted from victim (eg. Fail2ban)
- Announced as a bad guy on the internet
- Some services or web also took a list from blacklist database to create a filter (eg. Google)
- Reducing productivity (eg. When your mail provider ban your IP address because of some malicious traffic or illegal activity and you can’t send or receive an e-mail)

Impact of Bad Reputation



Impact of Bad Reputation



Mitigation of Bad Reputation

Mitigation of Bad Reputation

- We can mitigate and keep our IP reputation on the internet with some help with MikroTik RouterOS Firewall rules & feature or other firewall mechanism
- In this presentation, we will discuss about some example of firewall mechanism with MikroTik RouterOS Firewall rules & feature
- **Disclaimer**: All of firewall rules which I wrote in this presentation is just an example, you need to see your user behavior first before you apply some firewall rules on your firewall devices (either for MikroTik devices or your > $5000 firewall ☺) and actually by default some firewall has a secure configuration that can drop DOS/DDoS Attack but I will suggest you to adjust the configuration with your network behavior

Mitigation – Step 1
CLI Configuration

- **Block all private services from public area**

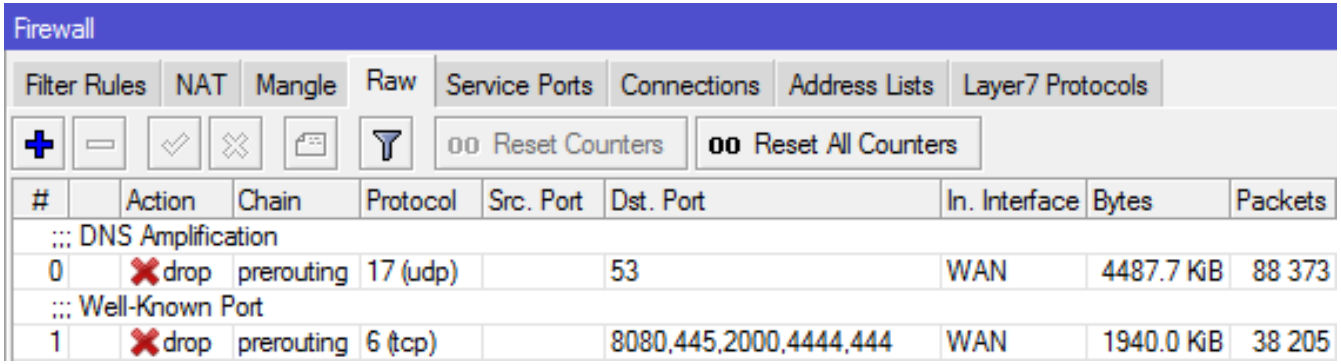
```
/ip firewall raw

add chain=prerouting in-interface=WAN action=drop
protocol=udp dst-port=53 comment="DNS
Amplification"

add chain=prerouting in-interface=WAN action=drop
protocol=tcp dst-port="8080,2000,22,23,80,53"
comment="Well-Known Port"
```

Objective: To **prevent** an Amplification attack, Denial of Services and Flooding to the internal devices either the Gateway Router

Mitigation – Step 1
Result & Winbox Configuration

- **Block all private services from public area**

Objective: To **prevent** an Amplification attack, Denial of Services and Flooding to the internal devices either the Gateway Router



Mitigation – Step 2
CLI Configuration

- **Block all well known virus port services from private network to the internet**

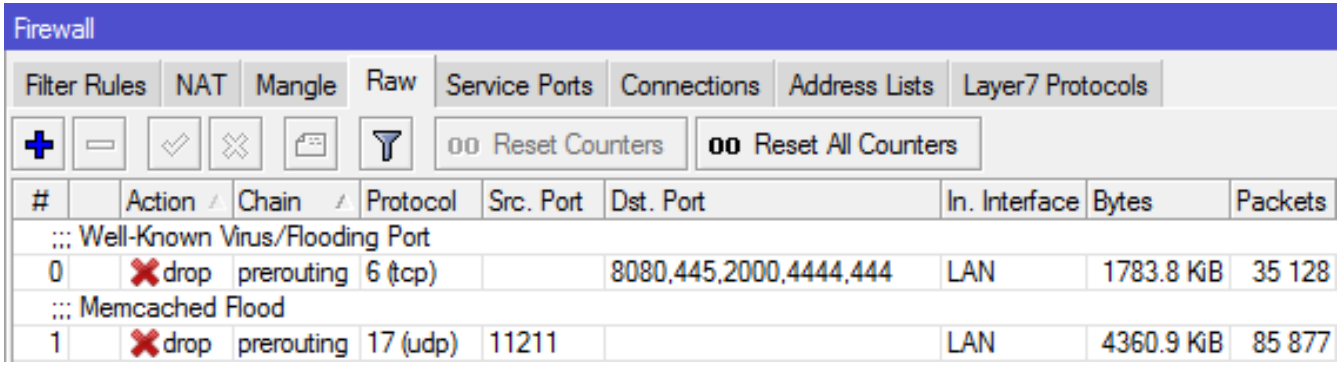
```
/ip firewall raw

add chain=prerouting in-interface=LAN action=drop
protocol=tcp dst-port="8080,445,2000, 4444,444"
comment="Well-Known Virus/Flooding Port"

add chain=prerouting in-interface=LAN action=drop
protocol=udp src-port="11211" comment="Memcached
Flood"
```

Objective: To **prevent** internal devices malicious/anomalies traffic to the internet or being botnet from Amplification Attack impact

Mitigation – Step 2
Result & Winbox Configuration

- **Block all well known virus port services from private network to the internet**

Objective: To **prevent** internal devices malicious/anomalies traffic to the internet or being botnet from Amplification Attack impact



Mitigation – Step 3
CLI Configuration

- **Gather Anomalies Connection**

```
/ip firewall filter

add action=add-src-to-address-list address-
list=dns-flood address-list-timeout=none-dynamic
chain=input comment="DNS Flood Gathering"
connection-limit=100,32 dst-port=53 in-
interface=LAN protocol=udp

add action=add-src-to-address-list address-
list=dns-flood address-list-timeout=none-dynamic
chain=forward comment="DNS Flood Gathering"
connection-limit=100,32 dst-port=53 in-
interface=LAN protocol=udp
```

Objective: To gather where internal devices that suspected from virus or botnet

Mitigation – Step 3
CLI Configuration

- **Gather Anomalies Connection**

```
/ip firewall filter

add action=add-src-to-address-list address-
list=smb-flood address-list-timeout=none-dynamic
chain=forward comment="SMB Flood Gathering"
connection-limit=100,32 dst-port=445 in-
interface=LAN protocol=tcp

add action=add-src-to-address-list address-
list=telnet-flood address-list-timeout=none-
dynamic chain=forward comment="Telnet Flood
Gathering" connection-limit=20,32 dst-port=23 in-
interface=LAN protocol=tcp
```

Objective: To gather where internal devices that suspected from virus or botnet

Mitigation – Step 3
CLI Configuration

- **Gather Anomalies Connection**

```
/ip firewall filter

add action=add-src-to-address-list address-
list=ssh-flood address-list-timeout=none-dynamic
chain=forward comment="SSH Flood Gathering"
connection-limit=20,32 dst-port=22 in-
interface=LAN protocol=tcp

add action=add-src-to-address-list address-
list=snpp-flood address-list-timeout=none-dynamic
chain=forward comment="SNPP/Backdoor Flood
Gathering" connection-limit=20,32 dst-port=444 in-
interface=LAN protocol=tcp
```

Objective: To gather where internal devices that suspected from virus or botnet

Mitigation – Step 3
CLI Configuration

- **Gather Anomalies Connection**

```
/ip firewall filter

add action=add-src-to-address-list address-
list=msf-indication address-list-timeout=none-
dynamic chain=forward comment="Metasploit
Indication" connection-limit=20,32 dst-port=4444
in-interface=LAN protocol=tcp

add action=log chain=forward comment="Abnormal
Traffic" connection-bytes=80000000 in-
interface=LAN log-prefix=Abnormal-Traffic
```

Objective: To gather where internal devices that suspected from virus or botnet

Mitigation – Step 3
Winbox Configuration

- **Gather Anomalies Connection**

Objective: To gather where internal devices that suspected from virus or botnet

Firewall

Filter Rules | NAT | Mangle | Raw | Service Ports | Connections | Address Lists | Layer7 Protocols

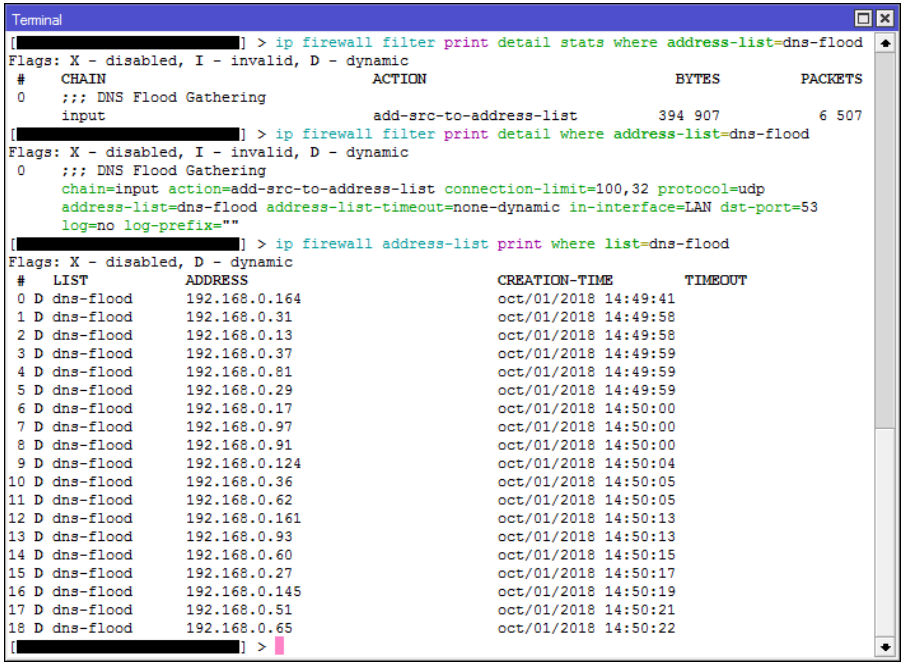
00 Reset Counters | 00 Reset All Counters

#	Action	Chain	Protocol	Dst. Port	In. Interface	Conn...	Conn...	Conn...	Log Prefix	Address List	Timeout	Bytes	Packets
;;; DNS Flood Gathering													
0	add src to address list	input	17 (udp)	53	LAN		100	32		dns-flood	none dynamic	0 B	0
;;; DNS Flood Gathering													
1	add src to address list	forward	17 (udp)	53	LAN		100	32		dns-flood	none dynamic	0 B	0
;;; SMB Flood Gathering													
2	add src to address list	forward	6 (tcp)	445	LAN		100	32		smb-flood	none dynamic	0 B	0
;;; Telnet Flood Gathering													
3	add src to address list	forward	6 (tcp)	23	LAN		20	32		telnet-flood	none dynamic	0 B	0
;;; SSH Flood Gathering													
4	add src to address list	forward	6 (tcp)	22	LAN		20	32		ssh-flood	none dynamic	0 B	0
;;; SNPP/Backdoor Flood Gathering													
5	add src to address list	forward	6 (tcp)	444	LAN		20	32		snpp-flood	none dynamic	0 B	0
;;; Metasploit Indication													
6	add src to address list	forward	6 (tcp)	4444	LAN		20	32		msf-indication	none dynamic	0 B	0
;;; Abnormal Traffic													
7	log	forward			LAN	80M			Abnormal-Traffic			0 B	0

Mitigation – Step 3 Result

- **Gather Anomalies Connection**

Objective: To gather where internal devices that suspected from virus or botnet

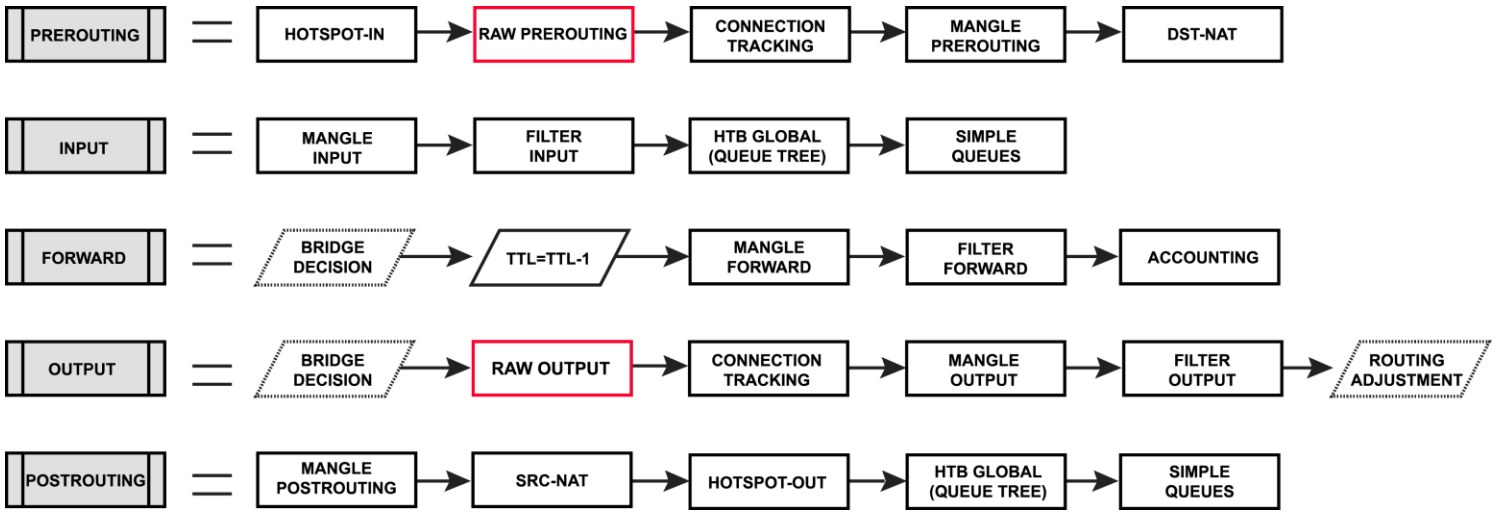


Mitigation Step 1 – 3 Note

- **`/ip firewall filter`** will **not PROCESSed** some rule if the PACKET already caught in **`/ip firewall raw`** and for some example is:

```
/ip firewall raw
add action=drop chain=prerouting dst-port=53
in-interface=WAN protocol=udp

/ip firewall filter
add action=drop chain=input dst-port=53
in-interface=WAN protocol=udp
```

Mitigation Step 1 – 3 Note



Mitigation Step 1 – 3 Note

```
[[redacted]] > ip firewall raw print detail
Flags: X - disabled, I - invalid, D - dynamic
 0    chain=prerouting action=drop in-interface=WAN dst-port=53 log=no log-prefix="" protocol=udp
[[redacted]] > ip firewall filter print detail
Flags: X - disabled, I - invalid, D - dynamic
 0    chain=input action=drop protocol=udp in-interface=WAN dst-port=53 log=no log-prefix=""
[[redacted]] > ip firewall raw print stats
Flags: X - disabled, I - invalid, D - dynamic
 #    CHAIN                                ACTION
 0    prerouting                           drop
[[redacted]] > ip firewall filter print stats
Flags: X - disabled, I - invalid, D - dynamic
 #    CHAIN                                ACTION
 0    input                                drop
[[redacted]] >
```

BYTES	PACKETS
10 764	207

BYTES	PACKETS
0	0

- You can see there, there is no packets or bytes stats for `/ip firewall filter` because UDP/53 to WAN already processed in `/ip firewall raw`

Mitigation Step 1 – 3 Note

Just Allow What You Needed ☺

(Drop All, Accept Few)

Mitigation – Step 4

- Log & alert any malicious traffic

You only need add two parameter on every firewall rules you make (related with step 3) with **log=yes** and **log-prefix=MALICIOUS** and for the alerting you can combine with log & alert management server (eg. Observium)

Objective: To log all of detected malicous traffic, so you can make a report or documentation monthly and alerting

Mitigation – Step 5

- You can torch your traffic daily or weekly
- You can check your flooder address-list daily
- Upgrade yourself and user security awareness
- Do routine update (antivirus, software, knowledge, username, password, etc.)
- If your internet using static IP, you also can check your IP reputation daily or weekly
- Avoid from using cracked or pirated software and operating system

Conlusion

Secure ≠ Easy

Feel so hard to detect any malicous traffic or keep your IP Reputation?

Let me help you!

michael@takeuchi.id

https://www.facebook.com/mict404

https://www.linkedin.com/in/michael-takeuchi/

g0tcha by AS38320?

please catch me up!

abuse@maxindo.net.id

Question & Answer

Slide is available in my github repository
https://github.com/mict404/slide/