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://www.dnsbl.info

etc.
Reputation Check (How it works?)

How it works?

Hey all of Blacklist Database Owner, is $IP$ listed on your database?

Hey all of Blacklist Database Owner, is $IP$ listed on your database?

Yes/No

Checker

Blacklist Database
Reputation Check
(Blacklist Database)

<table>
<thead>
<tr>
<th>IP Info</th>
<th>Whois</th>
<th>DNS</th>
<th>RBL</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Failed 0 out of 105 tests.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- access.redhawk.org
- all.spamblock.unit.liu.se
- b.barracudacentral.org
- bl.deadbeef.com
- bl.emailbasura.org
- bl.spamcannibal.org
- bl.spamcop.net
- blackholes.five-ten-sg.com
- blackholes.mail-abuse.org
- blacklist.sci.kun.nl
- blacklist.woody.ch
- bogons.cymru.com
- bsb.spamlookup.net
- cbl.abuseat.org
- cbl.anti-spam.org.cn
- cbl.less.anti-spam.org.cn
- cblplus.anti-spam.org.cn
- cd1.anti-spam.org.cn
- combined.njabl.org

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

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Length</th>
<th>Info</th>
<th>Protocol</th>
<th>Length</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS</td>
<td>75</td>
<td>Standard query response</td>
<td>DNS</td>
<td>75</td>
<td>Standard query response</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0x5bf2 No such name A</td>
<td></td>
<td></td>
<td>m35.ljxdqzu.com</td>
</tr>
<tr>
<td>DNS</td>
<td>75</td>
<td>Standard query</td>
<td>DNS</td>
<td>75</td>
<td>Standard query</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0xec9 A</td>
<td></td>
<td></td>
<td>m35.biqbitd.com</td>
</tr>
<tr>
<td>DNS</td>
<td>75</td>
<td>Standard query response</td>
<td>DNS</td>
<td>75</td>
<td>Standard query response</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0xd5a8 No such name A</td>
<td></td>
<td></td>
<td>m35.biqbitd.com</td>
</tr>
<tr>
<td>DNS</td>
<td>148</td>
<td>Standard query response</td>
<td>DNS</td>
<td>75</td>
<td>Standard query</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0xd5a8 No such name A</td>
<td></td>
<td></td>
<td>m35.biqbitd.com</td>
</tr>
<tr>
<td>DNS</td>
<td>75</td>
<td>Standard query response</td>
<td>DNS</td>
<td>75</td>
<td>Standard query</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0xec9a9 No such name A</td>
<td></td>
<td></td>
<td>m35.biqbitd.com</td>
</tr>
<tr>
<td>DNS</td>
<td>75</td>
<td>Standard query response</td>
<td>DNS</td>
<td>75</td>
<td>Standard query</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0x3e4e No such name A</td>
<td></td>
<td></td>
<td>m35.biqbitd.com</td>
</tr>
<tr>
<td>DNS</td>
<td>75</td>
<td>Standard query response</td>
<td>DNS</td>
<td>75</td>
<td>Standard query</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0x4d87 A</td>
<td></td>
<td></td>
<td>m35.aghpmy.com</td>
</tr>
<tr>
<td>DNS</td>
<td>148</td>
<td>Standard query response</td>
<td>DNS</td>
<td>75</td>
<td>Standard query</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0x4d87 No such name A</td>
<td></td>
<td></td>
<td>m35.aghpmy.com</td>
</tr>
<tr>
<td>DNS</td>
<td>75</td>
<td>Standard query response</td>
<td>DNS</td>
<td>75</td>
<td>Standard query</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0x3e4e No such name A</td>
<td></td>
<td></td>
<td>m35.aghpmy.com</td>
</tr>
<tr>
<td>DNS</td>
<td>75</td>
<td>Standard query response</td>
<td>DNS</td>
<td>75</td>
<td>Standard query</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0x7f1c A</td>
<td></td>
<td></td>
<td>m35.uksjnxz.com</td>
</tr>
<tr>
<td>DNS</td>
<td>75</td>
<td>Standard query response</td>
<td>DNS</td>
<td>75</td>
<td>Standard query</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0xbc91 A</td>
<td></td>
<td></td>
<td>m35.uksjnxz.com</td>
</tr>
<tr>
<td>DNS</td>
<td>148</td>
<td>Standard query response</td>
<td>DNS</td>
<td>75</td>
<td>Standard query</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0xbc91 No such name A</td>
<td></td>
<td></td>
<td>m35.uksjnxz.com</td>
</tr>
<tr>
<td>DNS</td>
<td>75</td>
<td>Standard query response</td>
<td>DNS</td>
<td>75</td>
<td>Standard query</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0x7f1c No such name A</td>
<td></td>
<td></td>
<td>m35.uksjnxz.com</td>
</tr>
<tr>
<td>DNS</td>
<td>75</td>
<td>Standard query response</td>
<td>DNS</td>
<td>75</td>
<td>Standard query</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0x97be A</td>
<td></td>
<td></td>
<td>m35.wdbltie.com</td>
</tr>
<tr>
<td>DNS</td>
<td>75</td>
<td>Standard query response</td>
<td>DNS</td>
<td>75</td>
<td>Standard query</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0x3519 A</td>
<td></td>
<td></td>
<td>m35.wdbltie.com</td>
</tr>
</tbody>
</table>
Spamming
Spamming

Brittany

MON JUN 25

Answer me back using the link and we can get acquainted. I would like to receive a lot of kisses! Lick all my pussy 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 source destined to the same target
- DDoS attacks are simultaneously launched from several sources destined to the same target

<table>
<thead>
<tr>
<th>DOS</th>
<th>DDoS</th>
</tr>
</thead>
<tbody>
<tr>
<td>One Attacker to One Target</td>
<td>Many Attacker to One Target</td>
</tr>
</tbody>
</table>
## Bruteforce Login

<table>
<thead>
<tr>
<th>Log</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apr/10/2018 16:58:27</td>
</tr>
<tr>
<td>Apr/10/2018 16:58:31</td>
</tr>
<tr>
<td>Apr/10/2018 16:58:33</td>
</tr>
<tr>
<td>Apr/10/2018 16:58:34</td>
</tr>
<tr>
<td>Apr/10/2018 16:58:38</td>
</tr>
<tr>
<td>Apr/10/2018 16:58:40</td>
</tr>
<tr>
<td>Apr/10/2018 16:58:42</td>
</tr>
<tr>
<td>Apr/10/2018 16:58:45</td>
</tr>
<tr>
<td>Apr/10/2018 16:58:47</td>
</tr>
<tr>
<td>Apr/10/2018 16:58:48</td>
</tr>
<tr>
<td>Apr/10/2018 16:58:52</td>
</tr>
<tr>
<td>Apr/10/2018 16:58:53</td>
</tr>
<tr>
<td>Apr/10/2018 16:58:55</td>
</tr>
<tr>
<td>Apr/10/2018 16:59:00</td>
</tr>
<tr>
<td>Apr/10/2018 16:59:01</td>
</tr>
<tr>
<td>Apr/10/2018 16:59:03</td>
</tr>
<tr>
<td>Apr/10/2018 16:59:06</td>
</tr>
<tr>
<td>Apr/10/2018 16:59:08</td>
</tr>
</tbody>
</table>
Notice of Claimed Infringement - Case ID

Evidentiary Information:
Protocol: BITTORRENT
Infringed Work: Transformers: The Last Knight
Infringing FileSize: 6377875658
Infringer's IP Address: 175.123.456.789
Infringer's Port: 1798
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

554 Your access to this mail system has been rejected due to the sending MTA's poor reputation. If you believe that this failure is in error, please contact the intended recipient via alternate means.
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

![Firewall Configuration](image_url)
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=\texttt{add-src-to-address-list} address-list=\texttt{smb-flood} address-list-timeout=\texttt{none-dynamic}
chain=\texttt{forward} comment="\texttt{SMB Flood Gathering}\"
connection-limit=100,32 dst-port=445 in-
interface=\texttt{LAN} protocol=\texttt{tcp}

add action=\texttt{add-src-to-address-list} address-list=\texttt{telnet-flood} address-list-timeout=\texttt{none-dynamic}
chain=\texttt{forward} comment="\texttt{Telnet Flood Gathering}\"
connection-limit=20,32 dst-port=23 in-
interface=\texttt{LAN} protocol=\texttt{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=8000000 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
Mitigation - Step 3

Result

- Gather Anomalies Connection

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

![Screen shot of network traffic and firewall settings]
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

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 malicious 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
Conclusion

Secure ≠ Easy
Feel so hard to detect any malicious 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
Thank you!

Slide is available in my github repository

https://github.com/mict404/slide/