Mikrotik: Block known viruses

If you want to stop (some of the) known viruses that always come in through the same port, add some rules to your Mikrotik firewall.

Paste this into Mikrotik terminal

```
/ip firewall filter
add chain=virus protocol=tcp dst-port=135-139 action=drop comment="Drop
Blaster Worm"
add chain=virus protocol=udp dst-port=135-139 action=drop comment="Drop
Messenger Worm"
add chain=virus protocol=tcp dst-port=445 action=drop comment="Drop Blaster
Worm"
add chain=virus protocol=udp dst-port=445 action=drop comment="Drop Blaster
Worm"
add chain=virus protocol=tcp dst-port=593 action=drop comment="________"
add chain=virus protocol=tcp dst-port=1024-1030 action=drop
comment="________"
add chain=virus protocol=tcp dst-port=1080 action=drop comment="Drop MyDoom"
add chain=virus protocol=tcp dst-port=1214 action=drop comment="________"
add chain=virus protocol=tcp dst-port=1363 action=drop comment="ndm
requester"
add chain=virus protocol=tcp dst-port=1364 action=drop comment="ndm server"
add chain=virus protocol=tcp dst-port=1368 action=drop comment="screen cast"
add chain=virus protocol=tcp dst-port=1373 action=drop comment="hromgrafx"
add chain=virus protocol=tcp dst-port=1377 action=drop comment="cichlid"
add chain=virus protocol=tcp dst-port=1433-1434 action=drop comment="Worm"
add chain=virus protocol=tcp dst-port=2745 action=drop comment="Bagle Virus"
add chain=virus protocol=tcp dst-port=2283 action=drop comment="Drop
Dumaru.Y"
add chain=virus protocol=tcp dst-port=2535 action=drop comment="Drop Beagle"
add chain=virus protocol=tcp dst-port=2745 action=drop comment="Drop
Beagle.C-K"
add chain=virus protocol=tcp dst-port=3127-3128 action=drop comment="Drop
MyDoom"
add chain=virus protocol=tcp dst-port=3410 action=drop comment="Drop
Backdoor OptixPro"
add chain=virus protocol=tcp dst-port=4444 action=drop comment="Worm"
add chain=virus protocol=udp dst-port=4444 action=drop comment="Worm"
add chain=virus protocol=tcp dst-port=5554 action=drop comment="Drop Sasser"
add chain=virus protocol=tcp dst-port=8866 action=drop comment="Drop
Beagle.B"
add chain=virus protocol=tcp dst-port=9898 action=drop comment="Drop
Dabber.A-B"
add chain=virus protocol=tcp dst-port=10000 action=drop comment="Drop
Dumaru.Y"
add chain=virus protocol=tcp dst-port=10080 action=drop comment="Drop
MyDoom.B"
```

```
add chain=virus protocol=tcp dst-port=12345 action=drop comment="Drop
NetBus"
add chain=virus protocol=tcp dst-port=17300 action=drop comment="Drop
Kuang2"
add chain=virus protocol=tcp dst-port=27374 action=drop comment="Drop
SubSeven"
add chain=virus protocol=tcp dst-port=65506 action=drop comment="Drop
PhatBot, Agobot, Gaobot"
add chain=forward action=jump jump-target=virus comment="jump to the virus
chain"
```

From:
https://wiki.plecko.hr/ - **Eureka Moment**

Permanent link:
https://wiki.plecko.hr/doku.php?id=mikrotik:scripting:block_known_viruses

Last update: **2019/10/31 09:05**