Блокировка ботов РКН

по мотивам этого поста от @ЗаТелеком и дополнений ниже

Если вы хотите заблокировать доступ к вашим ресурсам со стороны ботов РКН то, для начала, надо узнать кого блокировать. Репозиторий C24Be/AS_Network_List позволяет получить список сетей и IP адресов для блокировки.

Самый лучший вариант - если ваш сайт уже спрятан за Cloudflare (это бесплатно). Тогда вы можете просто добавить правило для блокировки конкретных сетей и обновление подсетей будет происходить автоматически. Если же вы предпочитаете другие варианты, то вы можете блокировать доступ на уровне сети, отдельного сервера или даже конкретного домена.

Примеры как блокировать:

- Cloudflare (предпочтительный, не требует обновлений)
- Mikrotik (требует ручного обновления)
- Juniper (требует ручного обновления)
- iptables (требует ручного обновления)
- nftables (требует ручного обновления)
- Nginx (можно настроить автоматическое обновление)

Cloudflare

Откройте панель настройки своего сайта в дашборде CF, перейдите по пунктам меню слева: Security -> WAF -> create rule -> edit expression и введите:

(ip.geoip.asnum in {61280 34500 51932 57835 197153 206684 216080})

Mikrotik

```
/ip firewall address-list
add address=185.224.228.0/22 list=fgup_grchc
add address=195.209.120.0/22 list=fgup_grchc
add address=212.192.156.0/22 list=fgup_grchc

/ip firewall filter
add action=reject chain=forward dst-address-list=fgup_grchc protocol=tcp
reject-with=tcp-reset
add action=drop chain=forward dst-address-list=fgup_grchc

/ip firewall raw
add action=drop chain=prerouting in-interface-list=WAN src-address-
list=fgup_grchc
```

Juniper

```
set firewall family inet filter BLOCK_GRCHC term TERM_BLOCK_GRCHC from
source-address 185.224.228.0/22
set firewall family inet filter BLOCK_GRCHC term TERM_BLOCK_GRCHC from
source-address 195.209.120.0/22
set firewall family inet filter BLOCK_GRCHC term TERM_BLOCK_GRCHC from
source-address 212.192.156.0/22
set firewall family inet filter BLOCK_GRCHC term TERM_BLOCK_GRCHC then
discard
set firewall family inet filter BLOCK_GRCHC term ALLOW_OTHERS then accept
set interfaces $IFTYPE unit $UNITNUM family inet filter input BLOCK_GRCHC
```

iptables

```
# drop grchc
-A PREROUTING -s 185.224.228.0/24 -j DROP
-A PREROUTING -s 185.224.229.0/24 -j DROP
-A PREROUTING -s 185.224.230.0/24 -j DROP
-A PREROUTING -s 185.224.231.0/24 -j DROP
-A PREROUTING -s 195.209.120.0/24 -j DROP
-A PREROUTING -s 195.209.121.0/24 -j DROP
-A PREROUTING -s 195.209.122.0/24 -j DROP
-A PREROUTING -s 195.209.123.0/24 -j DROP
-A PREROUTING -s 212.192.156.0/24 -j DROP
-A PREROUTING -s 212.192.157.0/24 -j DROP
-A PREROUTING -s 212.192.158.0/24 -j DROP
```

nftables

```
set GRCHC {
                type ipv4_addr
                elements = {185.224.228.0/24, 185.224.229.0/24,
185.224.230.0/24, 185.224.231.0/24, 195.209.120.0/24,
                195.209.121.0/24, 195.209.122.0/24, 195.209.123.0/24,
212.192.156.0/24, 212.192.157.0/24, 212.192.158.0/24}
                flags interval
}
chain input {
                type filter hook input priority 0; policy drop
                ip saddr @GRCHC counter drop
}
```

Nginx

Репозиторий со всеми нужными скриптами и инструкциями: freemedia-tech/nginx-rugov-block

Не забудьте настроить ежедневное обновление списков выполняя в кроне ./updateBlocklist.sh --restart