

Kdo nám to tu klepe na party?

tomas@vps1:~\$ whoami

- 18 let
- Student 4. (maturitního) ročníku na SSŠVT
- O technologie jsem se začal zajímat už během karantény (2020)
- Začal jsem s Pythonem, přešel později na C#
- Ve volném čase vyvíjím open source software
- Dnes se věnuji hlavně kyberbezpečnosti a sítím
- Pracoval jsem u společnosti AgentFly Technologies (která vyvíjí vojenské drony) jako vývojář
- Pracuji momentálně u společnosti ATS-Telcom Praha jako penetrační tester a vývojář



www.batacek.eu

O co šlo

Dva honeypoty – návnadové servery, které se tváří zranitelně a zaznamenávají, co se na nich kdo pokusí udělat. Stejný poskytovatel, stejná chvíle, jediný rozdíl: kolik toho bylo otevřené.

srv3

46 služeb

SMB, SSH, Telnet, web, databáze...
jako skutečné služby.

Málo portů, hodně detailu: hesla,
příkazy, stažené soubory.

srv4

65 535 portů

Odpovídá na všech TCP portech.
Hodně portů, málo detailu: z 95 %
jen čas, adresa a port.

Kdo to spravoval

Jazykový model

Oba honeypoty nasadil a měsíc
provozoval model (Opus 5 a Fable 5):
root, zadání a nikdo, kdo by radil.

Kontrola 2× týdně, pokaždé nový chat bez
paměti.

25 dní

analytické okno 22. 8. – 16. 9.

5,48 mil.

spojení

40 057

různých IP adres

123,8 GB

syrových dat za celý běh



batacek.eu/honeypot

Kdo pozdě zabezpečuje, sám sobě škodí

21. 8. 2026, čas UTC – srv4

22:26:29

22:36:03

22:48:29

Start

První spojení

srv4, port 6028/tcp

+9,5 min

První pokus o přihlášení

PostgreSQL (5432), uživatel postgres –
zatím bez hesla

+22 min

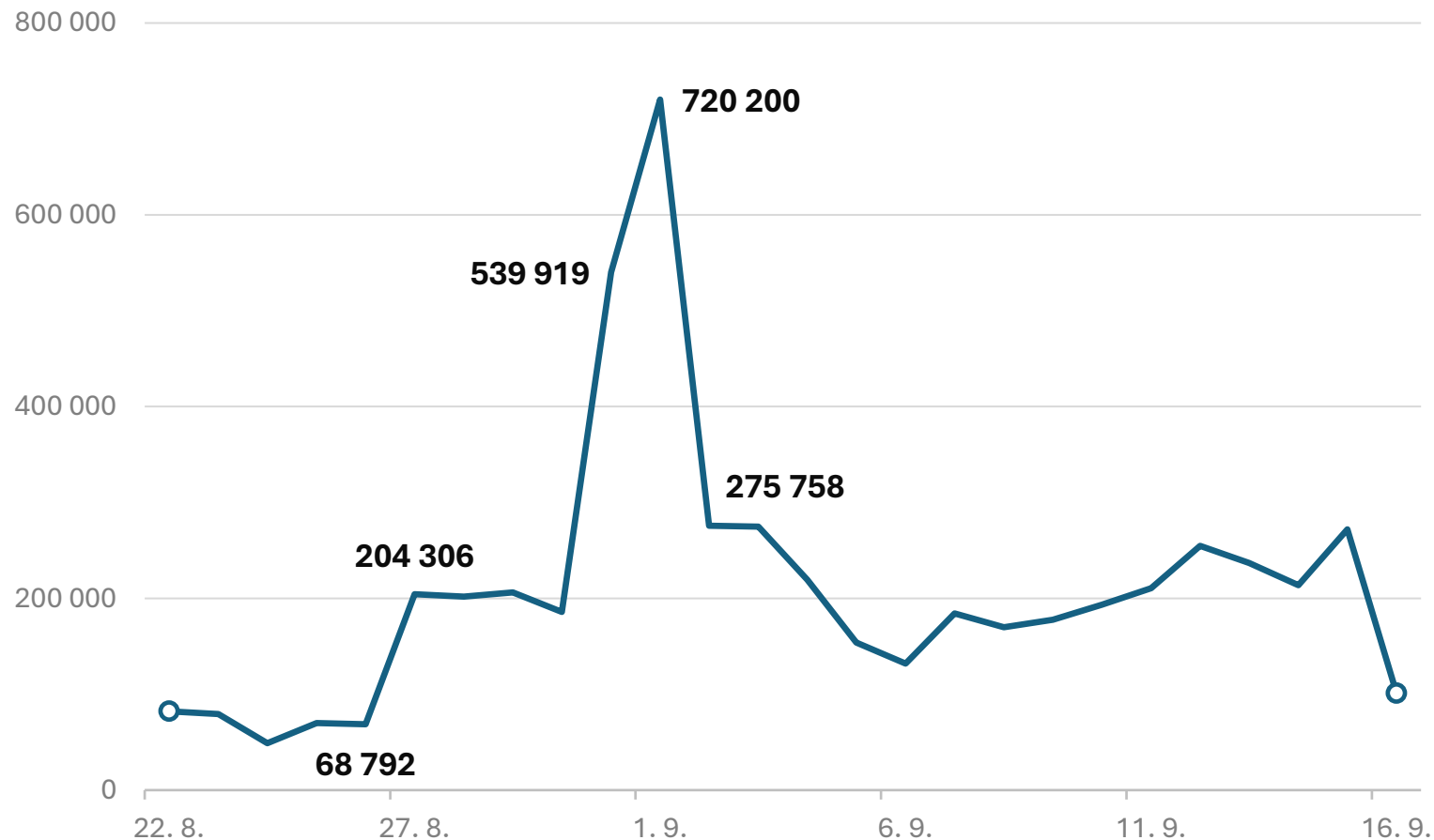
První jméno a heslo

SSH, root / 19840316. Hned za ním
slovníkový útok po sekundách:
3.1415926535, 19850702, 19840508...

22 minut od prvního spojení už někdo zkoušel heslo na root.

Celkový provoz

Spojení denně – oba servery dohromady, všechny porty



×3 přes noc

26. → 27. 8.: ze 69 tisíc na 204 tisíc spojení za den.

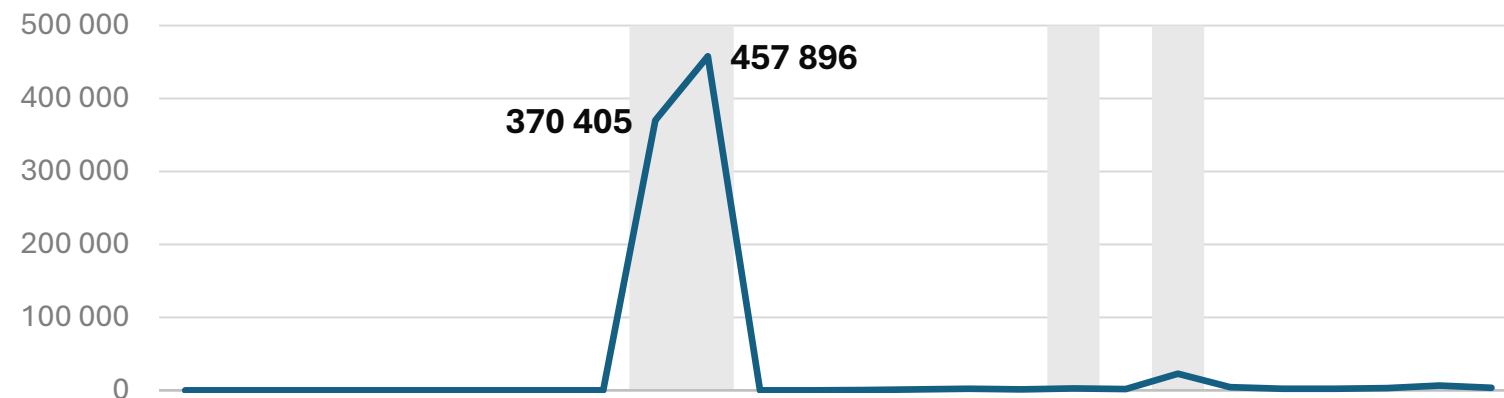
720 tisíc

spojení 1. 9. – desetkrát víc než o šest dní dřív.

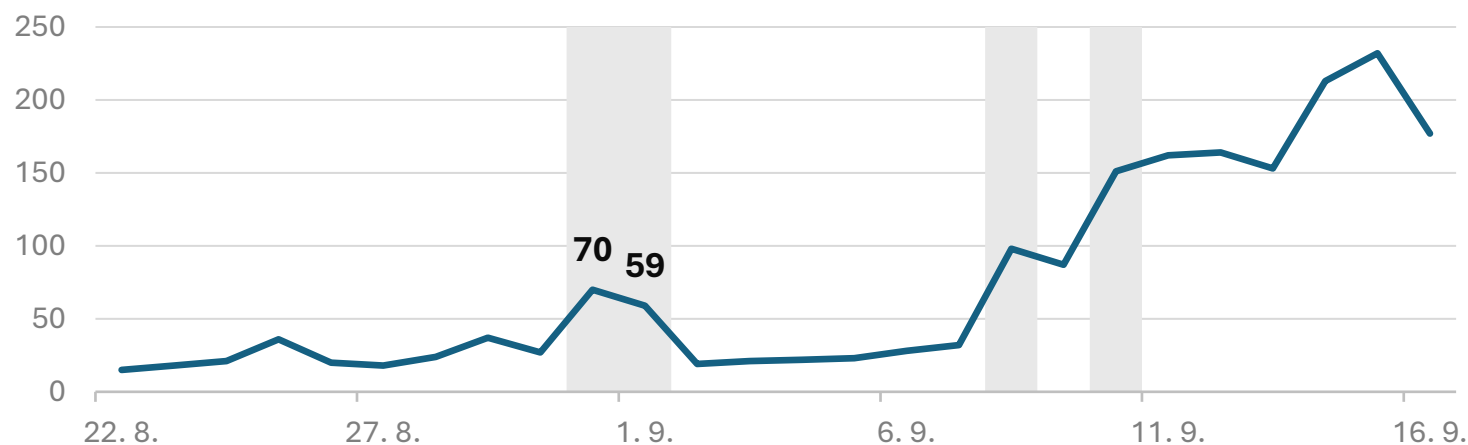
Ne, není to chyba v datech.

Co je to kampaň?

Spojení denně



Různých IP adres denně



Zdroj: honeypot srv3 + srv4, 22. 8. – 16. 9. 2026. Šedě dny, kdy na portu běžela kampaň.

828 tisíc

spojení na port 5901 (VNC) za dva dny, 31. 8. a 1. 9.

35 adres

je udělalo. Adres přitom přibylo jen pár desítek.

Kampaň

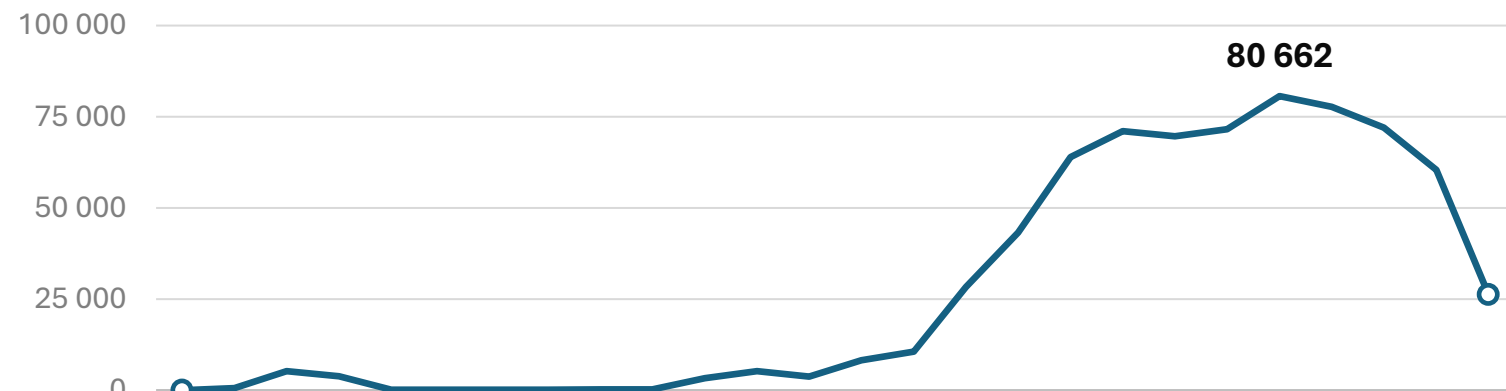
= IP adresa s aspoň **1 000 spojeními za den** na jednom serveru

–95 % / –4 %

spojení / útočníků na portu 5901, když se kampaň odfiltrují

A tohle kampaň není

Spojení denně na portu 5900



Různých IP adres denně na portu 5900



Zdroj: honeypot srv3 + srv4. Prázdný bod = první a poslední den okna jsou jen půlden (okno začíná a končí ve 12:00 UTC).

663 adres

za den na vrcholu 14. 9. Do konce srpna to byly desítky.

Pod prahem

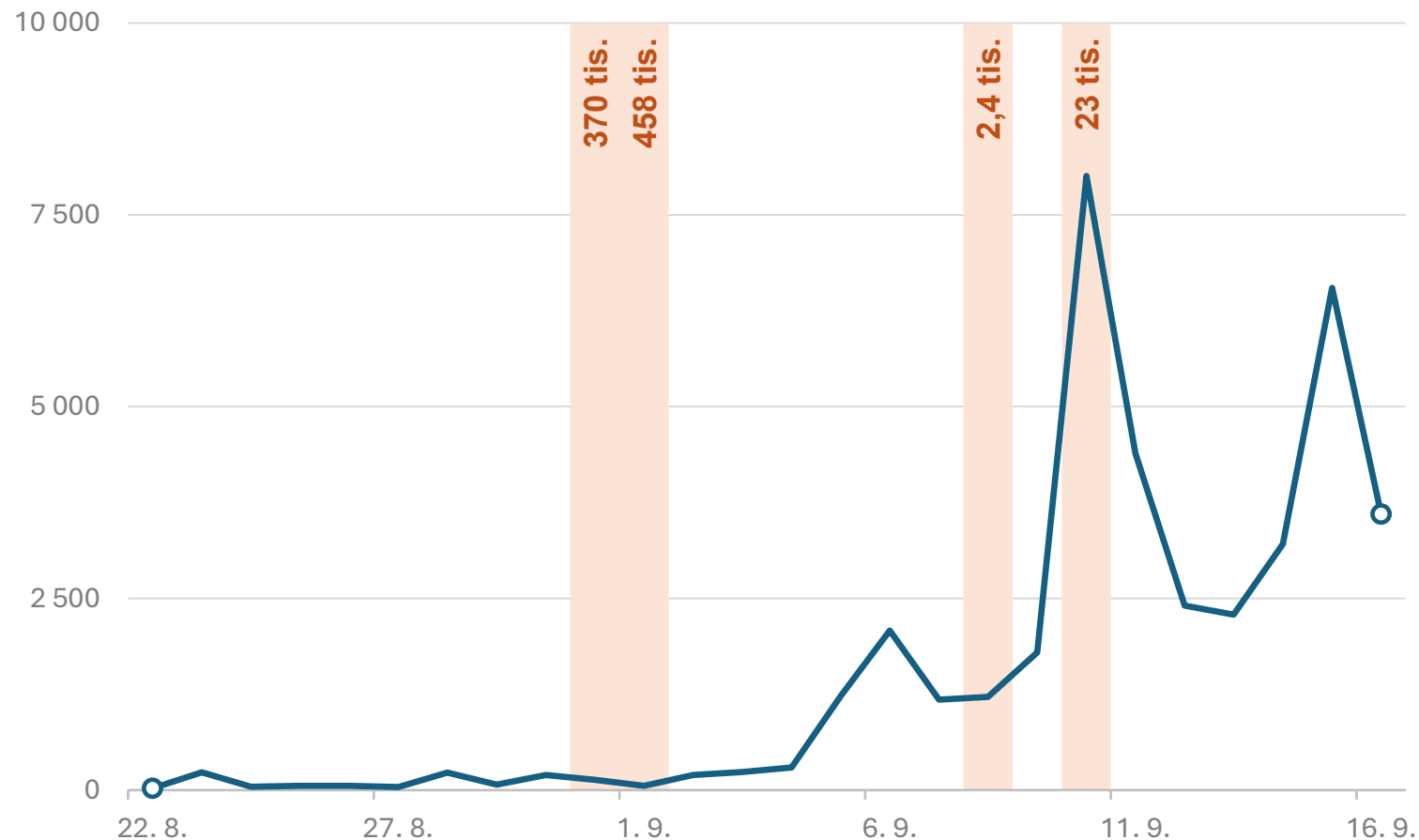
Stovky adres, skoro každá pod 1 000 spojeními za den. Pravidlo vlnu nechytí.

5901: spojení ↑, adresy skoro ne
→ **kampaň**

5900: spojení ↑ i adresy ↑
→ **skutečná změna**

Jak v grafech značím kampaně

Příklad: port 5901, spojení denně



Šum

Stabilní provoz bez kampaní.
Podle něj se řídí měřítko osy.

Den s kampaní

Kampaň do čáry nepočítám, jen ji vyznačím.

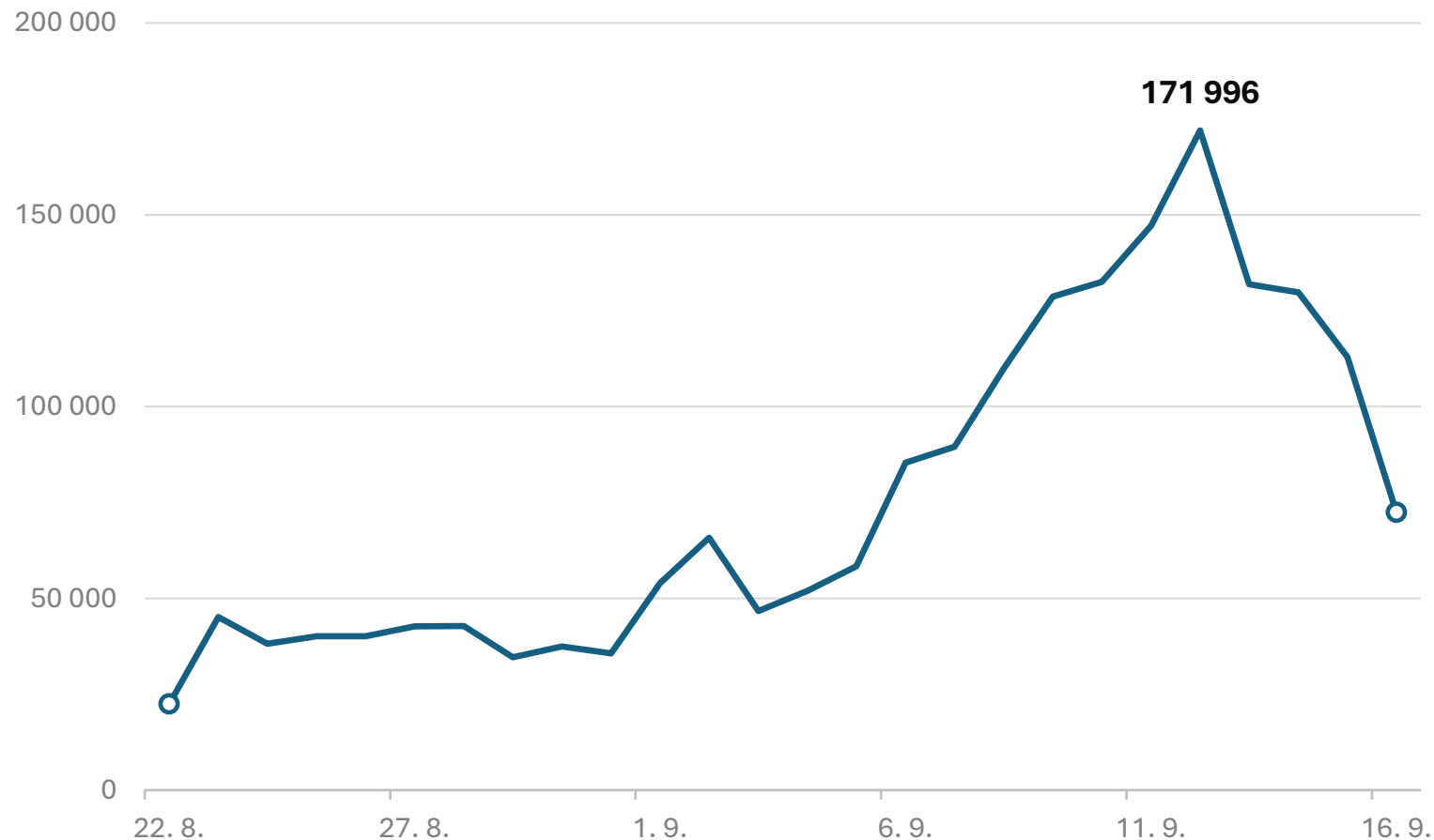
458 tis. Kolik to bylo i s kampaní

Celkový počet spojení toho dne.
Takové číslo by se do měřítka nevešlo.

Kampaň = IP adresa s aspoň 1 000 spojeními za den na jednom serveru.

Vyfiltrované kampaně

Šum – spojení denně bez kampaní, oba servery, všechny porty



64 %

všech spojení byly kampaně. V grafu už nejsou.

×3,5

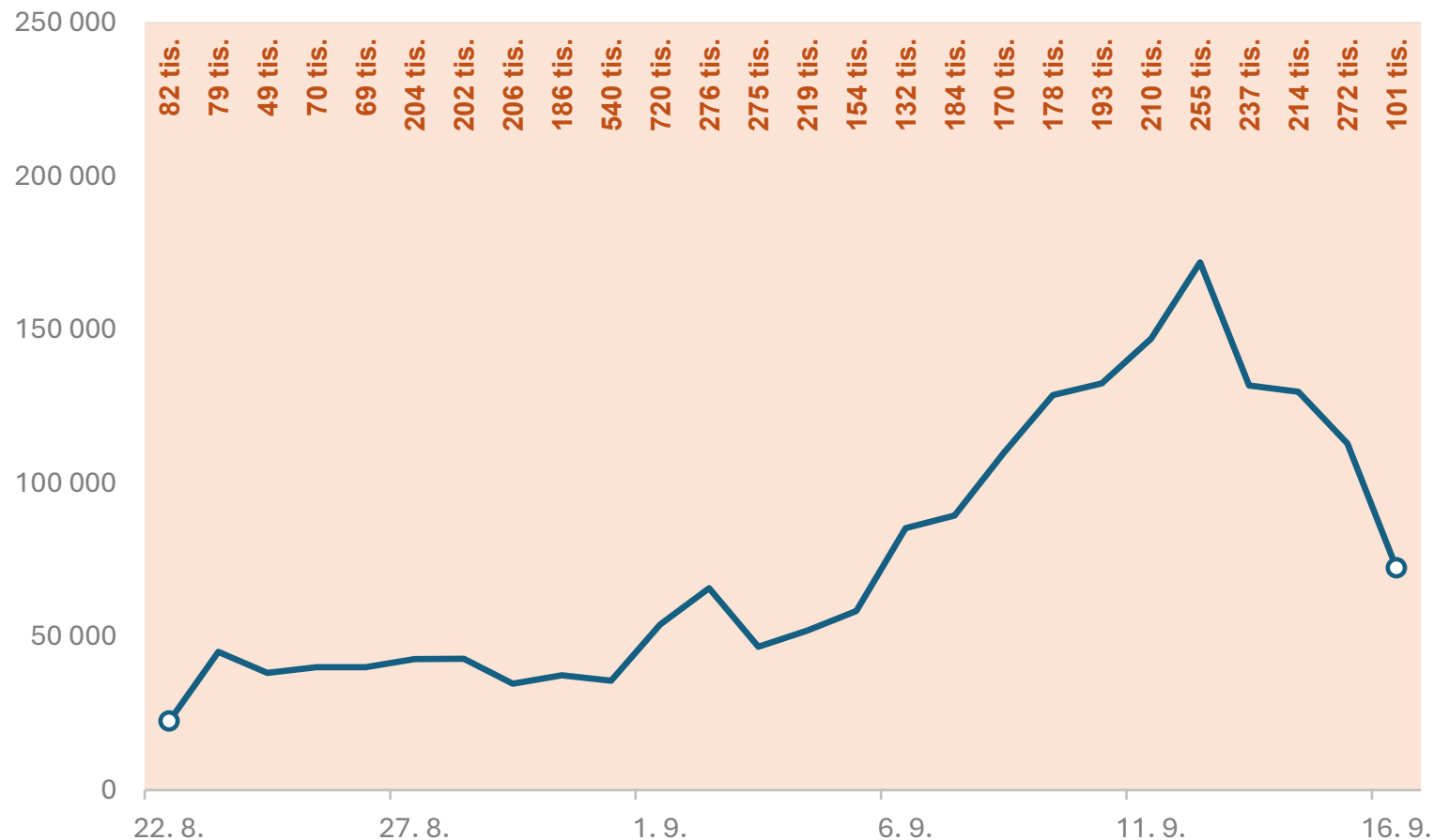
Šum od konce srpna do poloviny září:
z 35–43 tisíc na 113–172 tisíc spojení
denně.

~70 %

toho nárůstu dělá jediný port: VNC
5900.

Celkový provoz bez kampaní

Spojení denně – oba servery dohromady, všechny porty



Šum

Spojení bez kampaní. Podle něj se řídí měřítko osy.

Den s kampaní

Kampaň běžela každý den, proto je oranžový celý graf.

720 Kolik to bylo i s kampaní

Celkový počet spojení toho dne, v tisících.

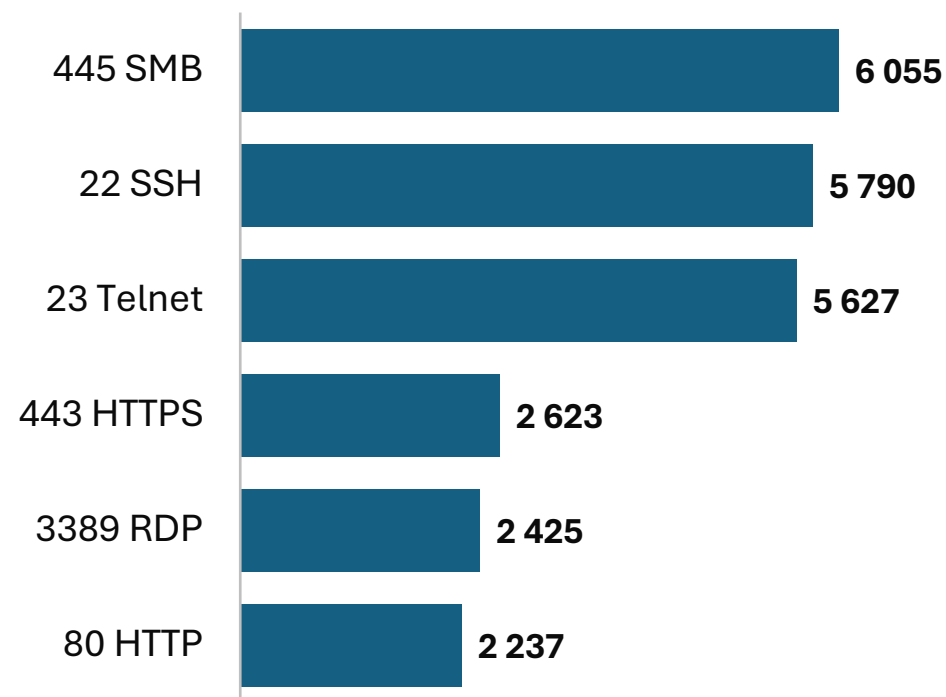
64 %

všech spojení byly kampaně.

Žebříček portů

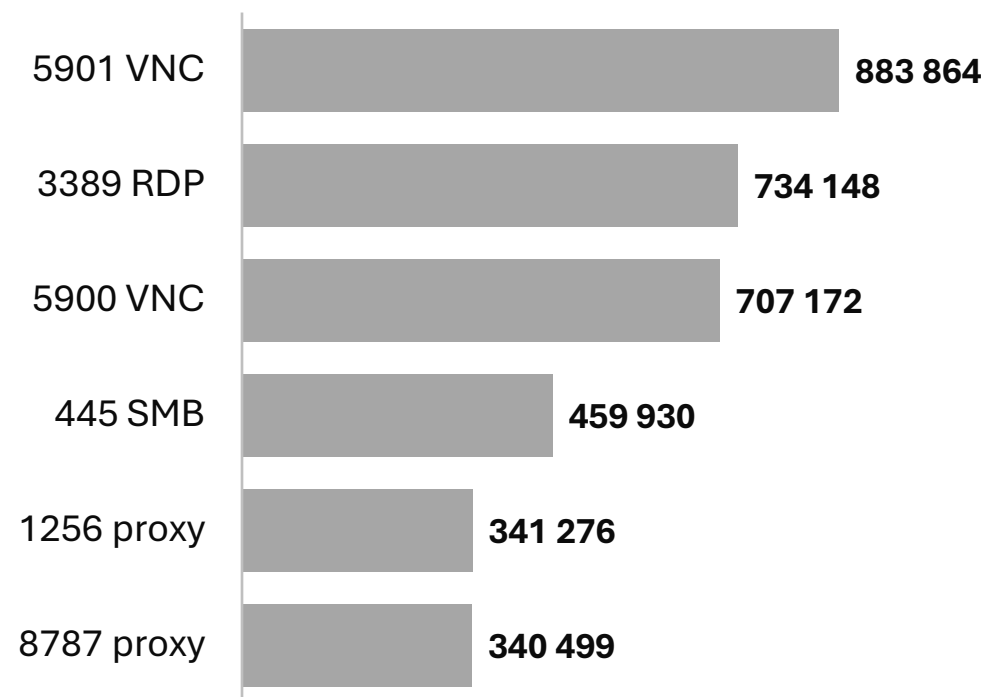
Podle počtu útočníků

různé IP adresy – včetně kampaní



Podle objemu

spojení – včetně kampaní

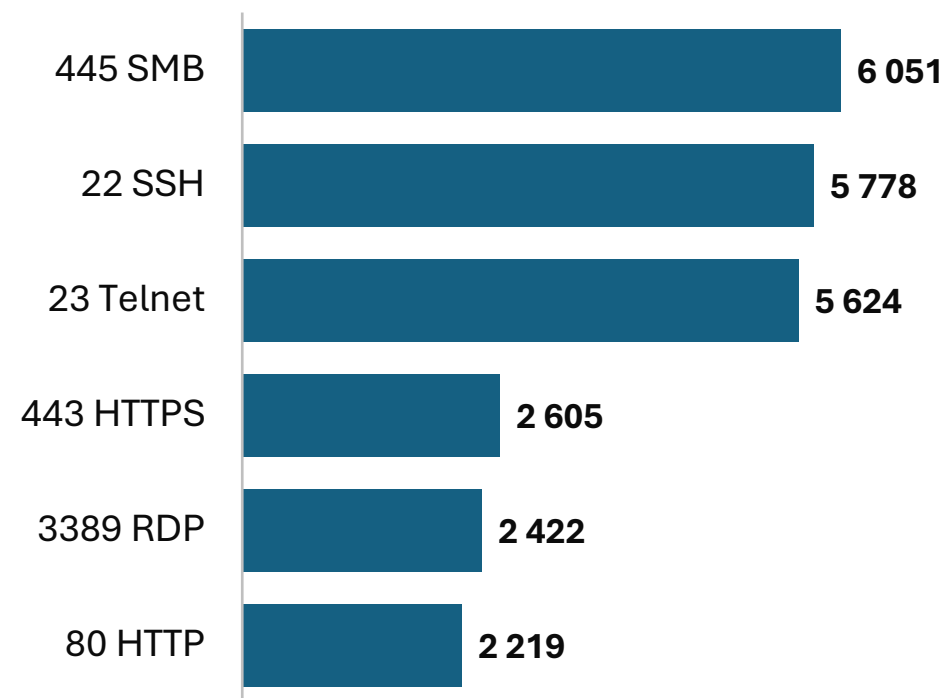


Objem táhne pár adres: porty 1256 a 8787 obsadilo dohromady jen 51 adres.

Žebříček portů bez kampaní

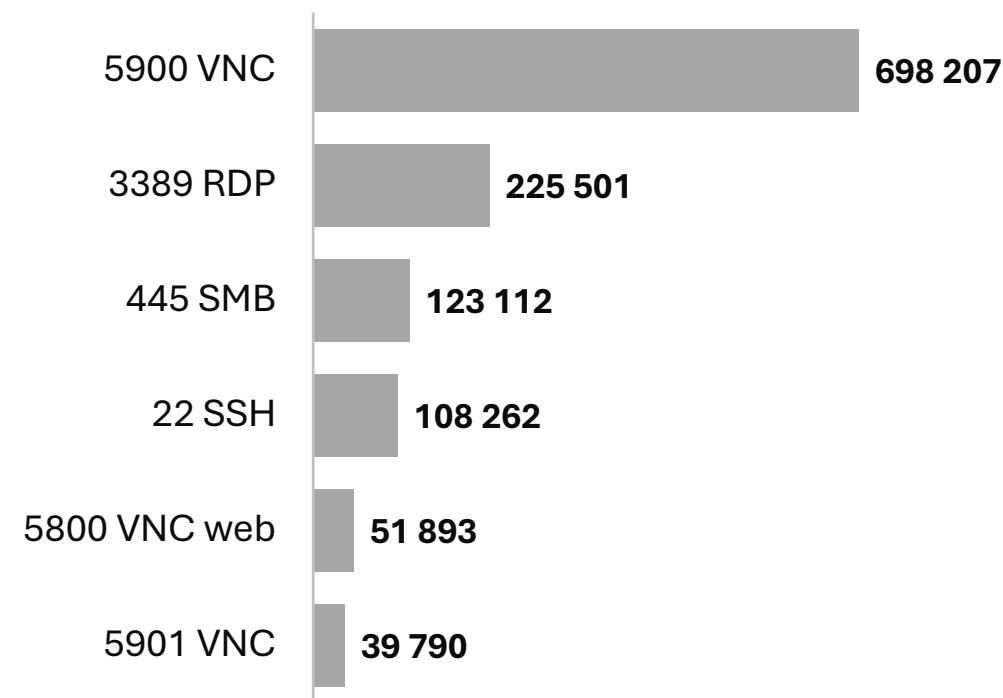
Podle počtu útočníků

různé IP adresy – bez kampaní



Podle objemu

spojení – bez kampaní

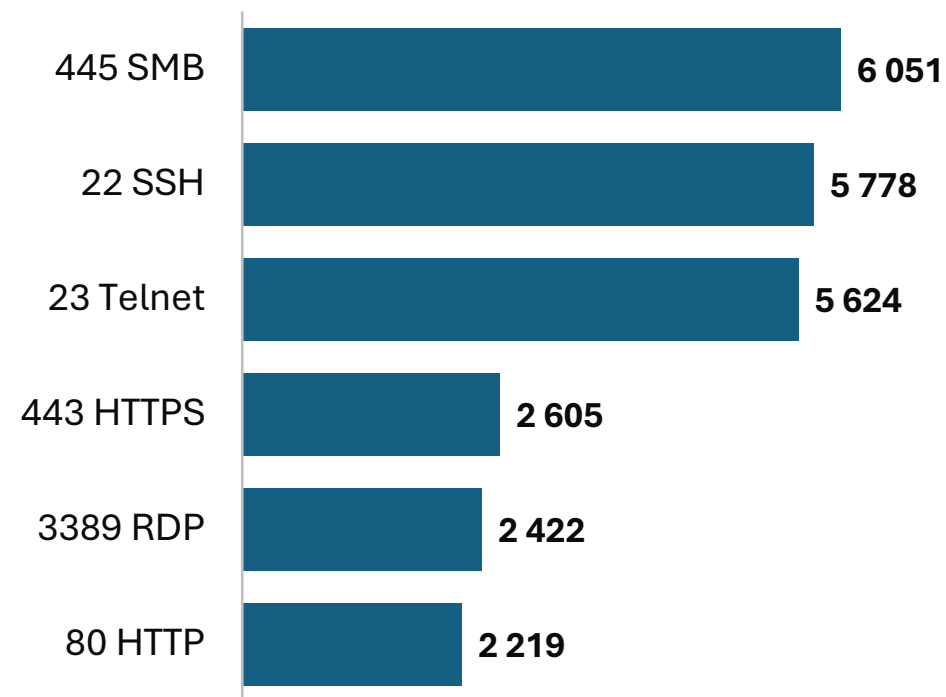


Pořadí útočníků se nepohne ani o místo. VNC 5900 ale vede dál – filtr mu ubral jen 1,3 %.

Bez kampaní a bez VNC vlny

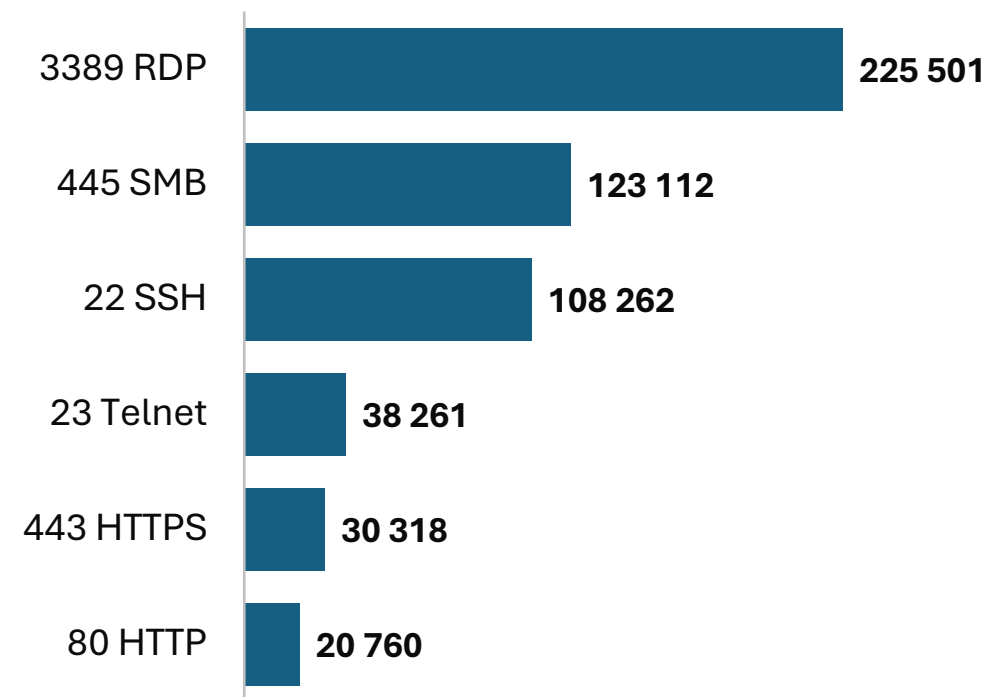
Podle počtu útočníků

různé IP adresy – bez kampaní a bez VNC



Podle objemu

spojení – bez kampaní a bez VNC

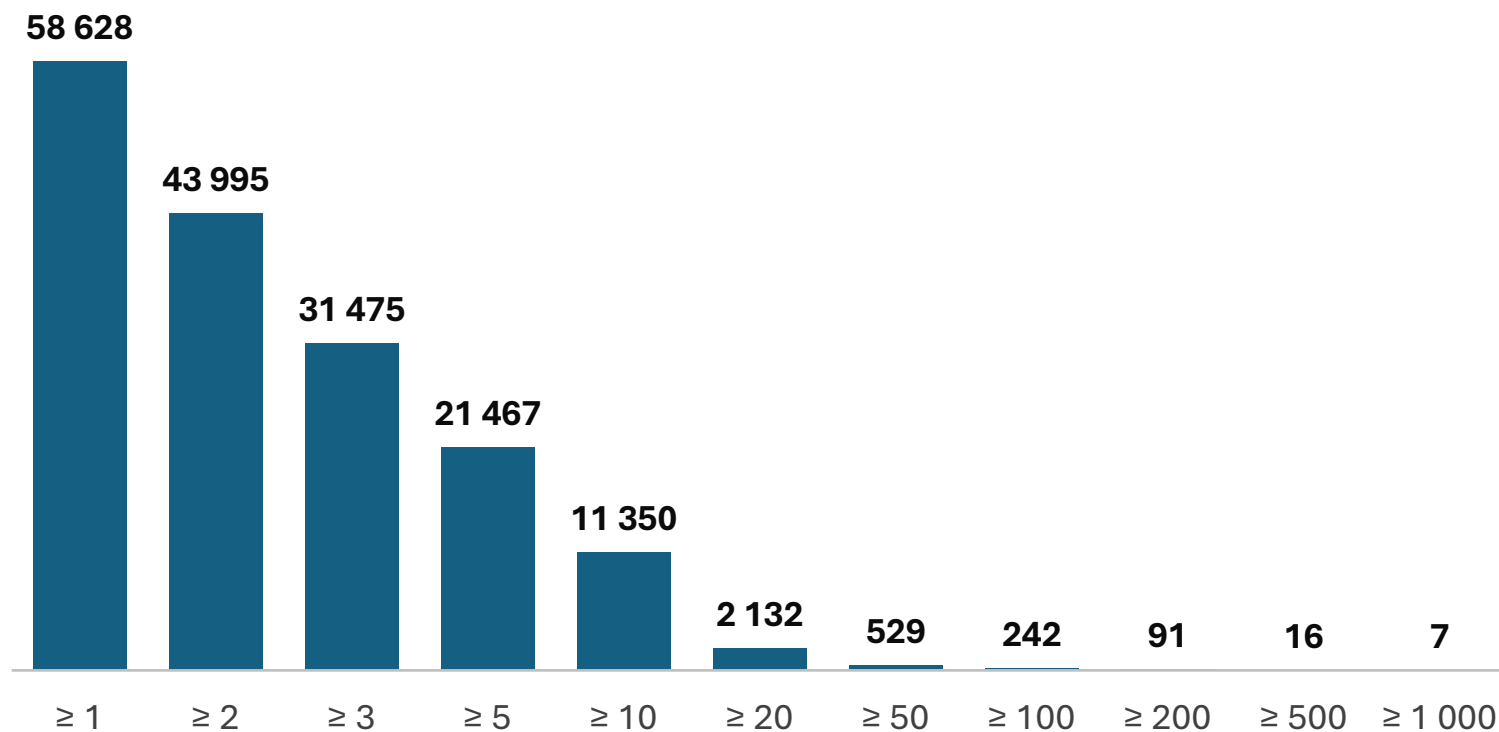


Obě metriky se shodnou na stejné šestici: SMB, SSH, Telnet, RDP, HTTPS, HTTP.

Kolik portů si někdo vyzkoušel?

Porty na srv4, které dostaly spojení od aspoň N různých IP adres

65 535 = celý rozsah portů



různých zdrojových IP adres na jeden port

89 %

všech portů dostalo za 25 dní aspoň jedno spojení.

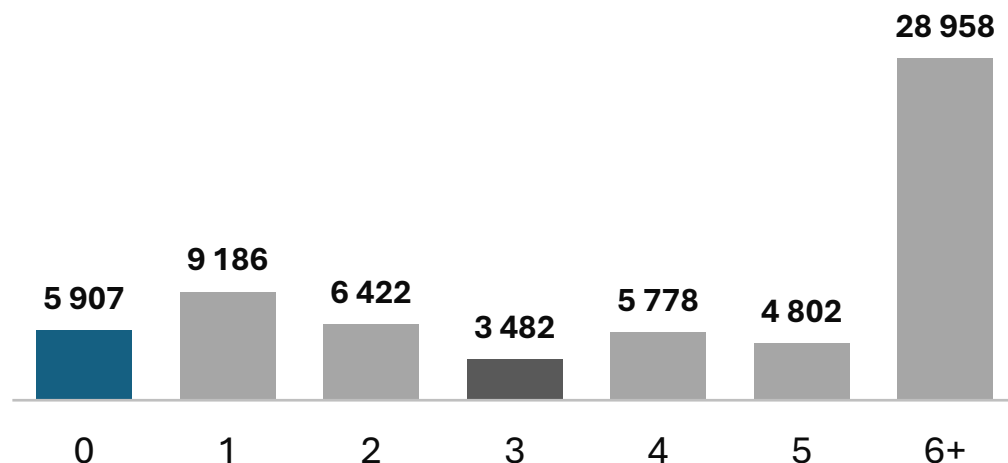
55 adres

prošlo každá přes 1 000 různých portů. Bez nich by pokrytí bylo jen 48 %.

O jaké porty se nikdo nezajímá?

Kolik spojení dostal jeden port

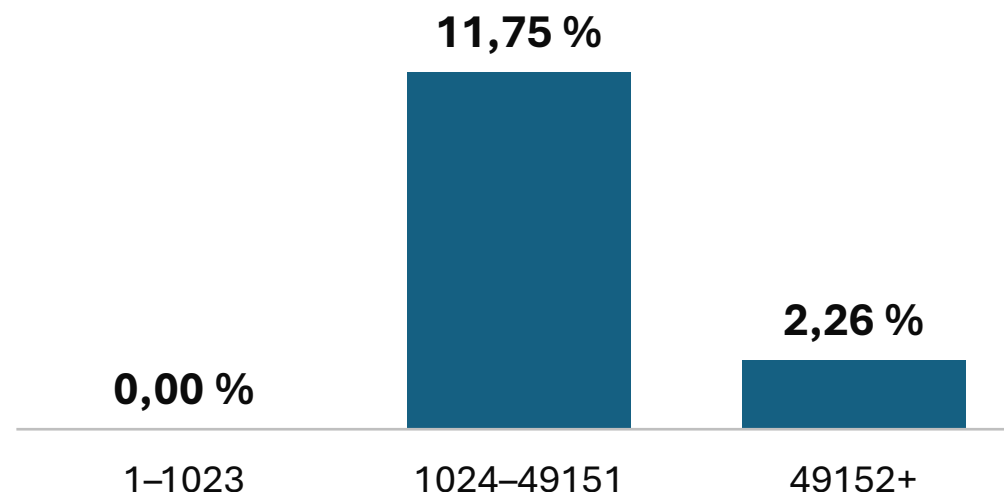
počet portů na srv4 za 25 dní



5 907 portů (9,15 %) nedostalo ani jedno spojení. **Propad u trojky:** nad 49 000 má 3 218 portů přesně 4 spojení, ale jen 60 přesně 3 – otisk průchodů celým rozsahem.

Kde se mlčí

podíl portů bez jediného spojení

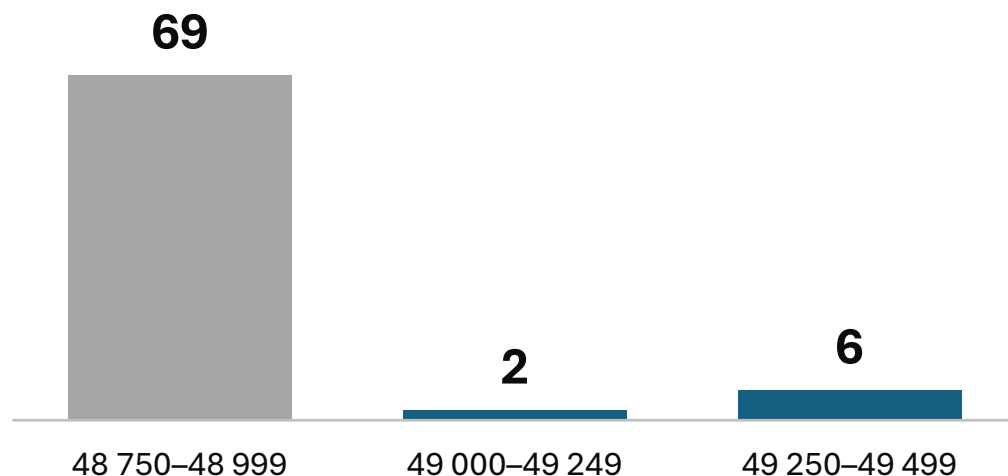


Ze systémových portů ani jeden – nejméně navštívené 318, 418, 426 a 457 měly po jednom spojení. **Nejvíc mlčí střed:** kolem 40–49 tisíc 20–35 % portů.

Porty se neskenují náhodně

Hrana na 49 000

portů bez spojení z 250 v každém úseku

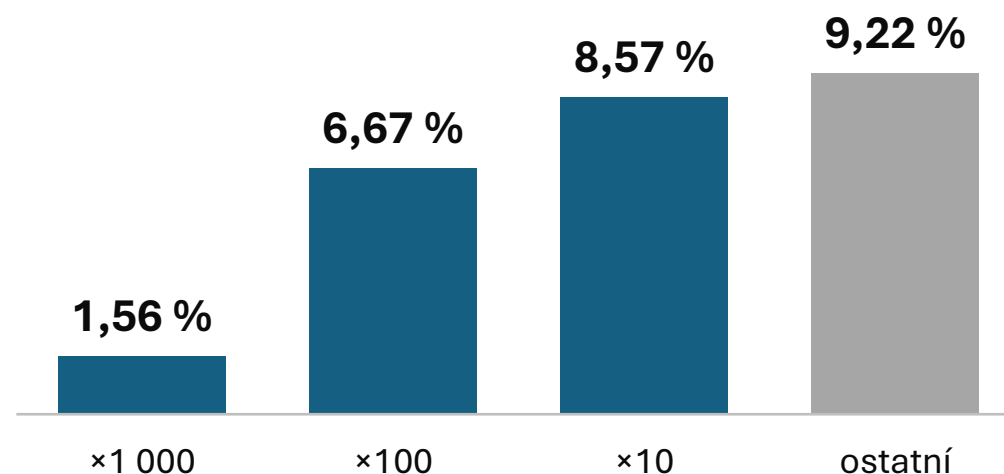


Skenery začínají na kulatém 49 000, ne na hranici IANA 49 152.

Medián spojení na port skočí na hraně ze 2 na 8. Lidsky nastavený rozsah, ne standard.

Kulatá čísla

podíl portů bez spojení podle toho, jak je číslo kulaté

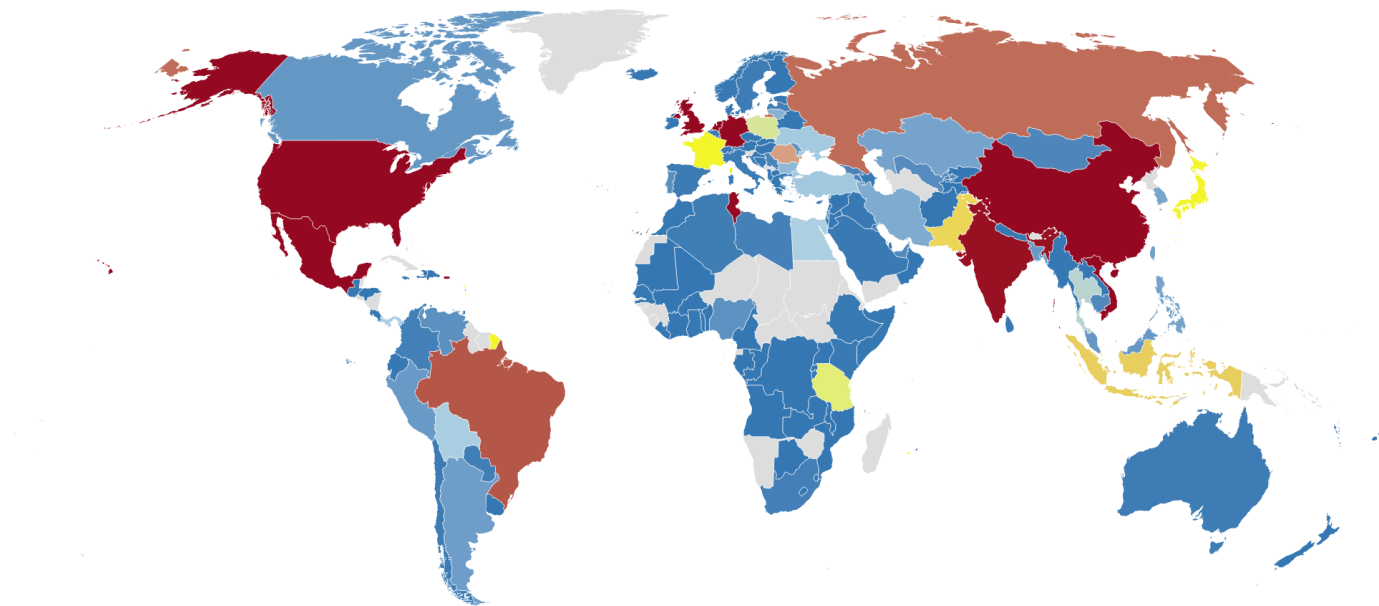


Čím kulatější číslo, tím spíš ho někdo zkusí. Z násobků tisícovky zůstal bez spojení jediný: 46000.

Bez vzoru: poslední číslice (8,6–9,8 % nul, v mezích šumu) a shluky nul (nejdelší souvislý úsek má jen 6 portů).

Příchozí spojení podle země

0 25 000 50 000



Vytvořeno nástrojem Datawrapper

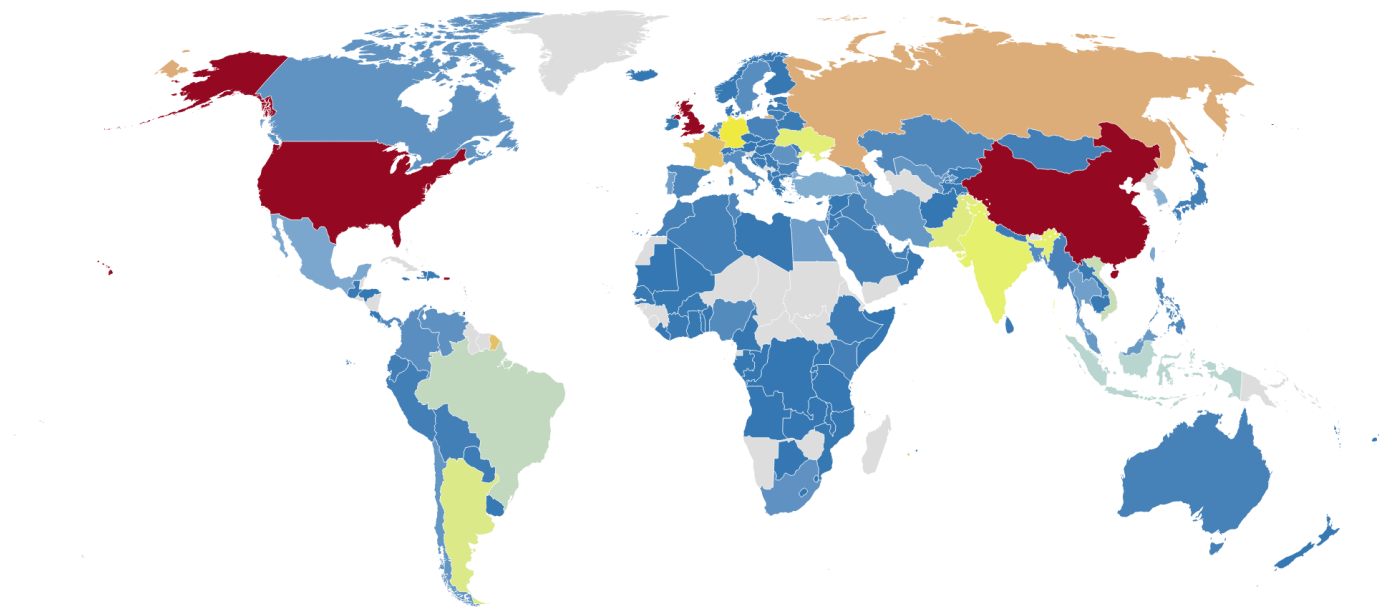
#	Země	Podíl	Spojení
1	USA	37,6 %	2 057 660
2	Německo	22,5 %	1 230 744
3	Čína	10,2 %	556 778
4	Velká Británie	8,9 %	486 870
5	Seychely	3,4 %	184 746
6	Nizozemsko	2,2 %	120 671
7	Tunisko	1,8 %	96 601
8	Vietnam	1,2 %	64 512
9	Mexiko	1,1 %	59 561
10	Indie	0,9 %	49 705

Německo je druhé kvůli jedinému poskytovateli: 84 % německých spojení přišlo z Contaba, ze 168 adres – od stejného poskytovatele, u kterého běžely naše honeypoty.

Zdroj: honeypot srv3 + srv4, 22. 8. – 16. 9. 2026, všechna spojení včetně kampaní. Země podle registrace IP adresy, ne podle polohy útočníka. Škála mapy končí na 50 000 spojení – státy nad ní mají nejtmaší barvu.

Útočící IP adresy podle země

0 1 000 2 000



Vytvořeno nástrojem Datawrapper

#	Země	Podíl	IP adres
1	USA	34,0 %	13 624
2	Čína	14,2 %	5 671
3	Velká Británie	7,2 %	2 870
4	Rusko	3,6 %	1 428
5	Francie	3,3 %	1 318
6	Hongkong	3,1 %	1 223
7	Německo	2,8 %	1 111
8	Indie	2,1 %	850
9	Ukrajina	2,1 %	827
10	Pákistán	2,0 %	798

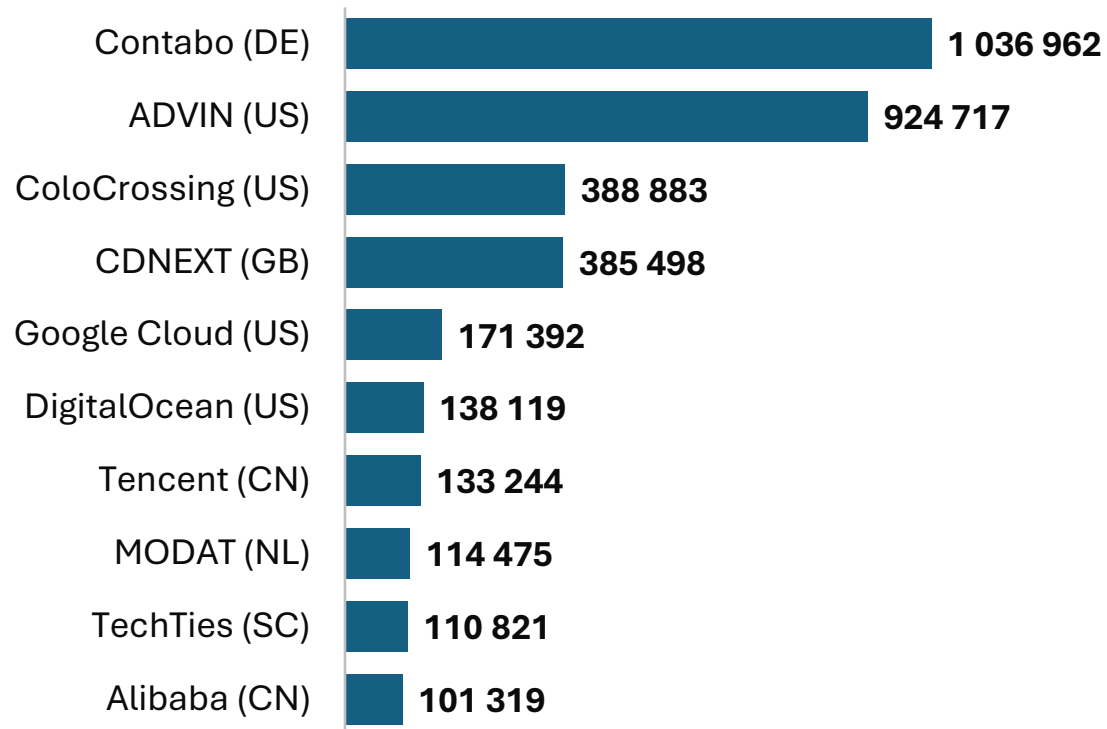
USA a Čína mají dohromady 48 % všech útočících adres. Německo spadne podle adres z druhého místa na sedmé.

Zdroj: honeypot srv3 + srv4, 22. 8. – 16. 9. 2026, 40 057 různých IP adres. Země podle registrace IP adresy, ne podle polohy útočníka. Škála mapy končí na 2 000 adres – státy nad ní mají nejtmavší barvu.

Největší sítě (ASN)

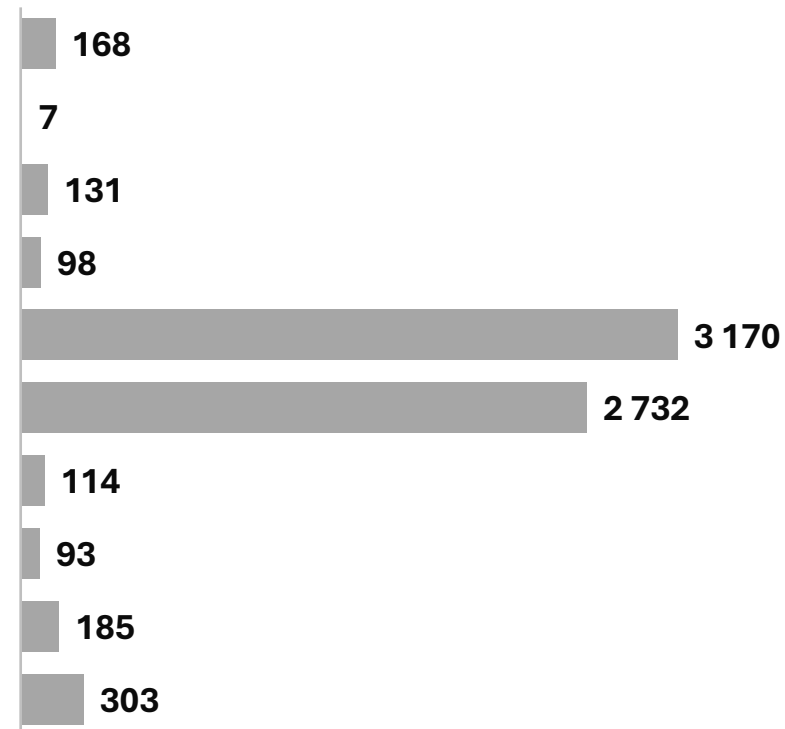
Spojení

deset sítí s největším počtem spojení



Z kolika IP adres

stejně sítě, stejné pořadí



Deset sítí udělalo 64 % všech spojení. ADVINT: 925 tisíc spojení ze 7 adres. Samé hostinky a cloudy – útoky nechodí ze zemí, ale z pronajatých serverů.

Zdroj: honeypot srv3 + srv4, 22. 8. – 16. 9. 2026, všechna spojení včetně kampaní. ASN podle databáze ip2asn; v závorce země registrace sítě.

Jména a hesla

Nejzkoušenější jména

počet pokusů o přihlášení

root	43 470
admin	10 909
enable	2 938
user	2 100
sa	2 049
support	1 551
test	1 518
ubuntu	1 456
cloud	1 281
postgr...	1 198

Nejčastější kombinace

jméno / heslo

#	Jméno	Heslo	Pokusů	IP adres
1	root	(prázdné)	3 084	219
2	admin	admin	2 649	849
3	enable	linuxshell	1 955	24
4	admin	(prázdné)	1 939	69
5	root	xc3511	1 591	76
6	root	admin	1 529	160
7	root	vizxv	1 523	120
8	root	123456	1 207	142
9	support	support	990	129
10	enable	system	983	27

xc3511 a vizxv jsou tovární hesla kamer a rekordérů ze slovníku botnetu Mirai. Zkoušeli i jména odvozená z adresy serveru: cloud, batacek, srv.

Zdroj: honeypot srv3 + srv4, 22. 8. – 16. 9. 2026, 25 217 různých kombinací. Jména enable a hesla linuxshell/system přišla s koncovým nulovým bajtem (\x00).

Co dělali po přihlášení

Nejčastější příkazy v emulovaném shellu

#	Příkaz	Počet	Relací
1	<code>uname -s -v -n -r -m</code>	41 470	41 470
2	<code>system</code>	21 144	21 143
3	<code>shell</code>	21 044	21 044
4	<code>sh</code>	21 015	21 014
5	<code>enable</code>	20 259	20 258
6	<code>linuxshell</code>	18 836	18 834
7	<code>echo -e "\x47\x41\x59\x46\x47\x54"</code>	4 749	493
8	<i>skript: uname, architektura, uptime, CPU, GPU...</i>	4 333	4 332
9	<code>/bin/busybox</code>	3 149	312
10	<code>/bin/./uname -s -v -n -r -m</code>	2 275	2 275

Kde to jsem?

`uname`: architektura a jádro, aby věděli, jaký binární soubor stáhnout.

enable → system → shell → sh

Sekvence botnetu Mirai: z menu zařízení se dostat do shellu. Asi 21 tisíc relací.

CPU a GPU

4 332 relací zjišťovalo procesor a grafickou kartu – typicky kvůli těžbě.

Co si odnést

22 min

Na internetu nejste neviditelní.

První heslo na root přišlo 22 minut po prvním spojení a 89 % všech portů někdo za 25 dní zkusil. Nestandardní port není úkryt.

64 %

Objem nedělají útočníci, ale pár adres.

Tolik spojení byly kampaně. Kdo se dívá jen na objem, vidí VNC a kontrolu proxy – ne to, na co se útočí.

6 služeb

Útočníci jdou pořád po stejném.

SMB, SSH, Telnet, RDP, HTTPS a HTTP. Když se odečtou výkyvy, shodne se na nich počet útočníků i objem.

Děkuji za pozornost



batacek.eu/honeypot

Zdroje

Všechna data v této prezentaci pocházejí z mých dvou honeypotů.

Žádná externí data o útocích nebyla použita.

Data	honeypoty srv3 a srv4, 21. 8. – 17. 9. 2026 (analyzováno 22. 8. – 16. 9.)
Pomocné nástroje	přiřazení IP adres k zemím a sítím: databáze ip2asn · mapy: Datawrapper
Vše ke stažení	data, metodika, skripty a záznam práce agentů: batacek.eu/honeypot