ComSource

Jak zvládat volumetrické útoky

Petr Kadlec, ComSource

Co je volumetrický útok?

Průměrná cena DDoS útoku je cca 25 dolarů za hodinu.

Princip

- Abnormální síťový provoz
  - Na konkrétní službu či síťový prvek
  - Na celou infrastrukturu
- Negativní dopady
  - Vyčerpání systémových prostředků serverů
  - Vyčerpání systémových prostředků síťových prvků
  - Vyčerpání kapacity datových tras
  - Vyčerpání kapacity internetového připojení
- Výsledek
  - Nefunkční služba
  - Přetížená infrastruktura
  - Nedostupný internet

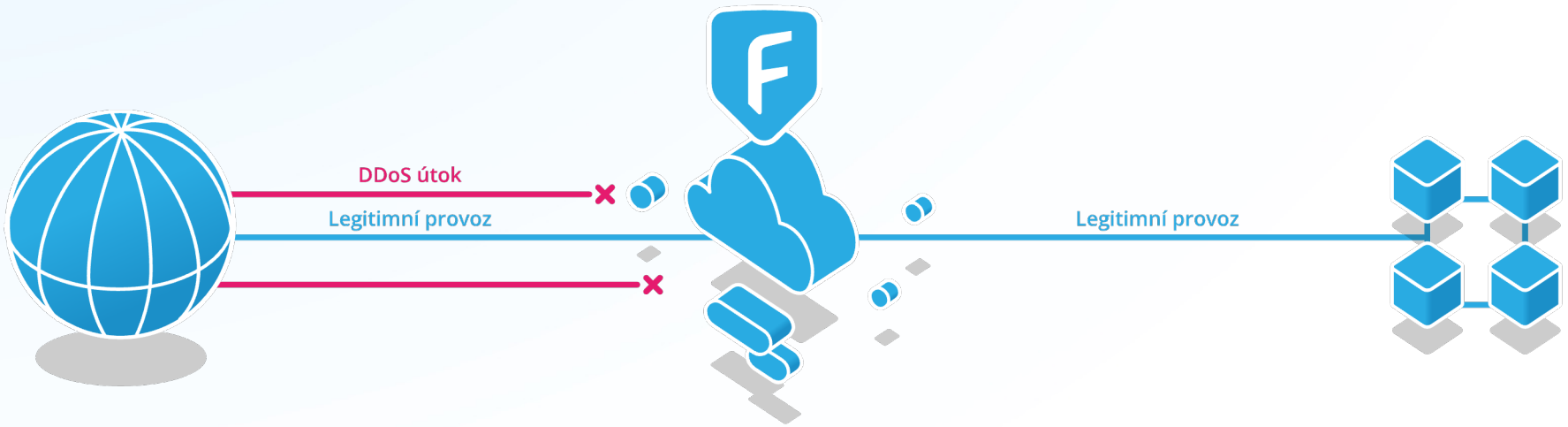
Motiv

- Finanční zisk
  - Až zaplatíte přestaneme
  - Když nezaplatíte, budeme útok opakovat
- Nefunkční služby
  - Konkurenční boj
  - Politický boj
- Maskování jiné činnosti
  - Maskování chytrého útoku
  - Zaměstnání personálu
  - Vyřazení bezpečnostních a monitorovacích systémů přetížením
- Vandalismus

Strategie obrany

Prevence	Ochrana	Obětování	Analýza
• Robustní infrastruktura • Minimální terč • Výkon a propustnost • Limitace systémových prostředků • Krizové plány a postupy • FENIX	• Filtrace v cloudu (FlowGuard) • CPE zařízení pro filtraci (hybridní filtrace) • Dodatečné náklady	• Blokace (RTBH, Flowspec) • Lepší jeden za všechny než všichni za jednoho • Předchozí domluva s dodavateli konektivity	• Vyhodnocení útoku a obrany • Definice a implementace opatření

Princip ochrany



ComSource

Trendy dalšího vývoje

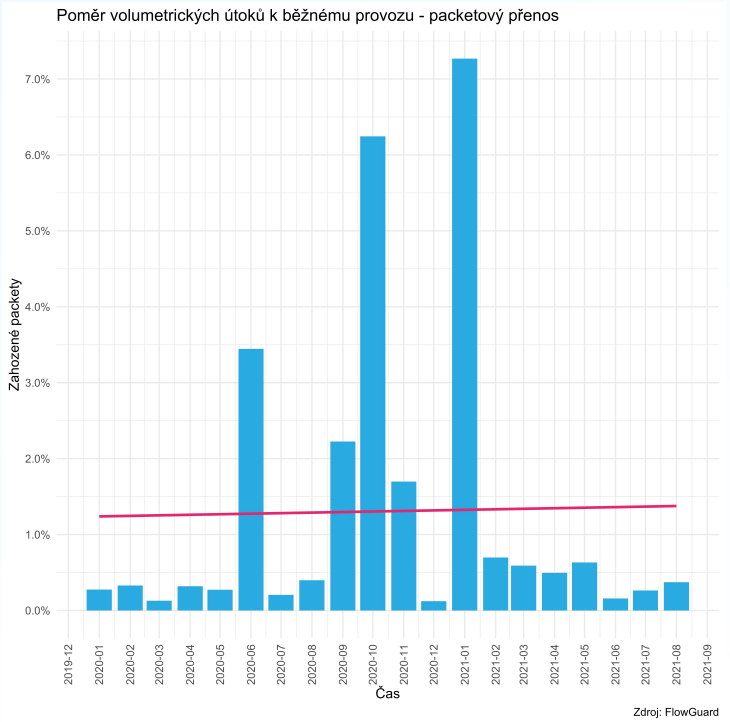
Začlenění AntiDDoS do obecné security

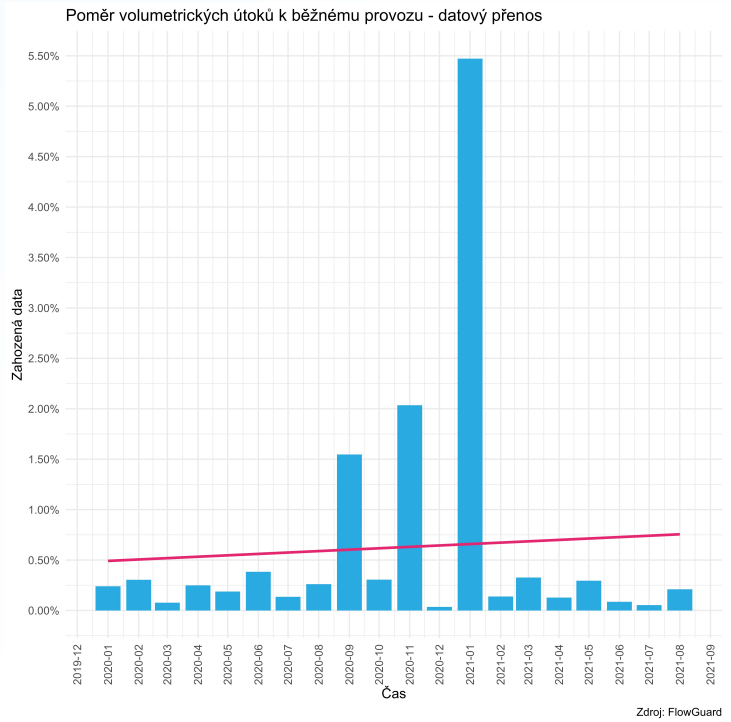
- Sdílení informací, integrace s MISP
- Klasifikace a korelace bezpečnostních (DDoS) incidentů
- Import informací do SIEM
- Import informací do SOAR

Automatizace správy sítě

- Využití provozních dat
- Využití dat o bezpečnostních incidentech
- Aplikace playbooků pro změny konfigurace síťových prvků
- Definice stupňů obrany a automatické přecházení mezi nimi

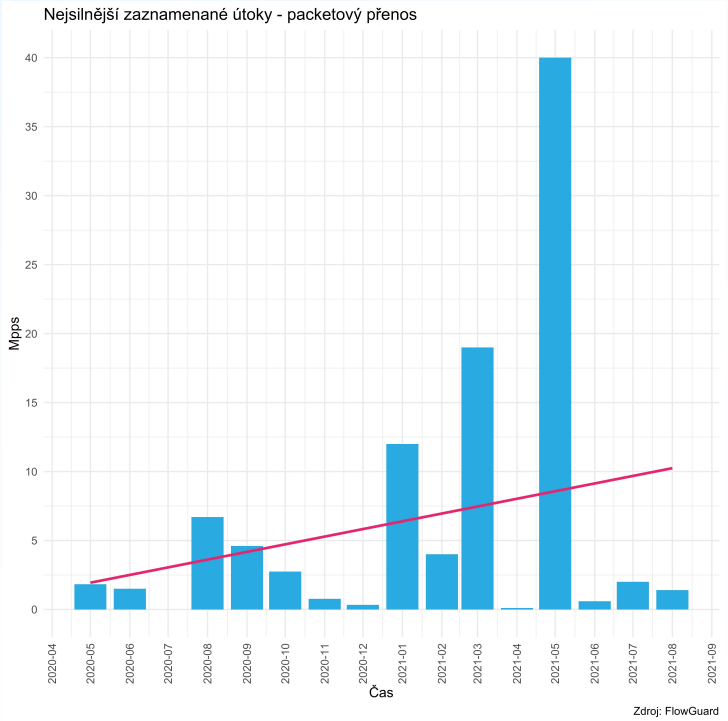
Trend růstu intenzity útoků

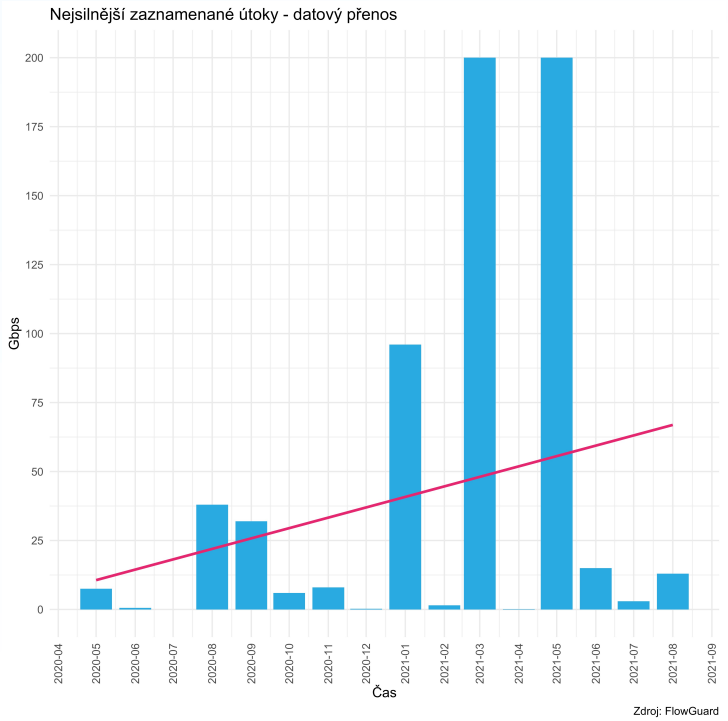




Com Source

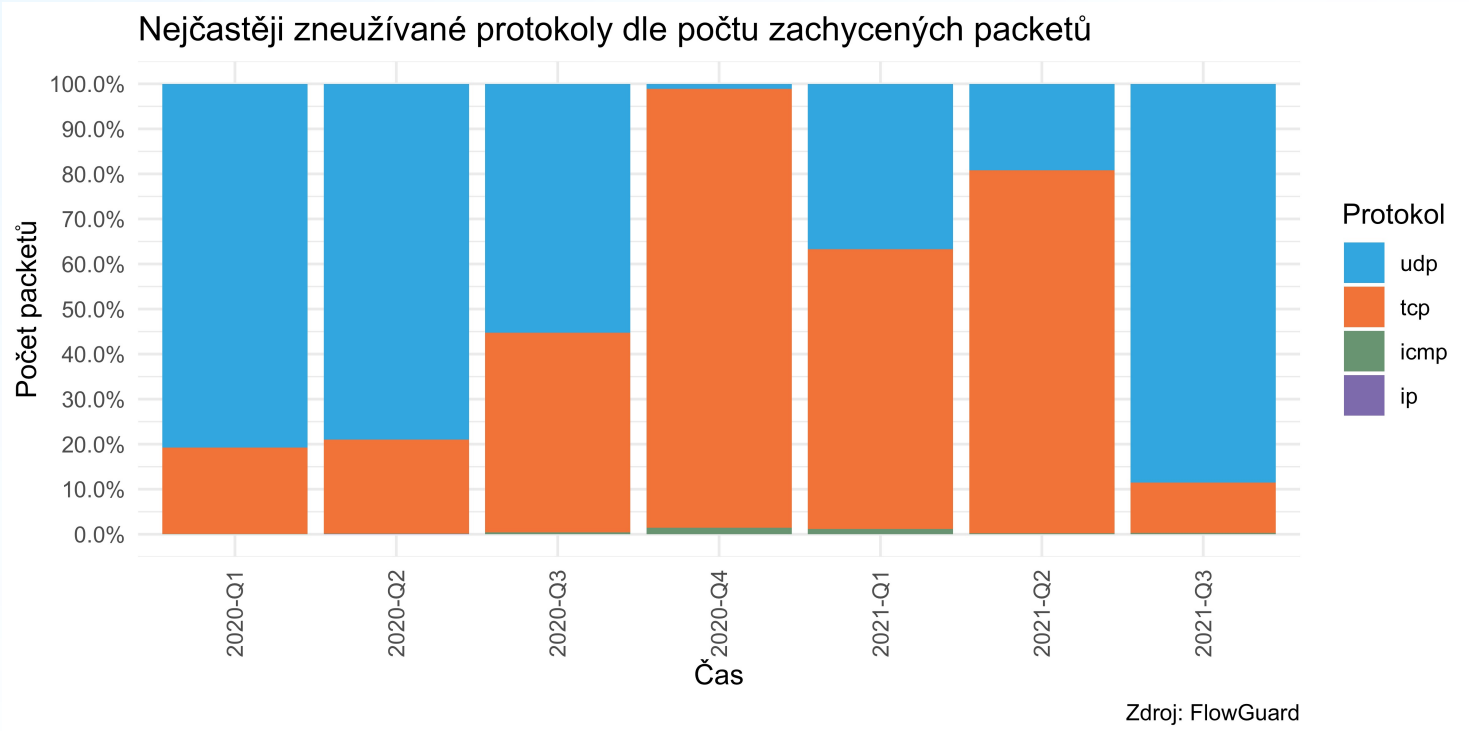
Nejsilnější zaznamenané útoky





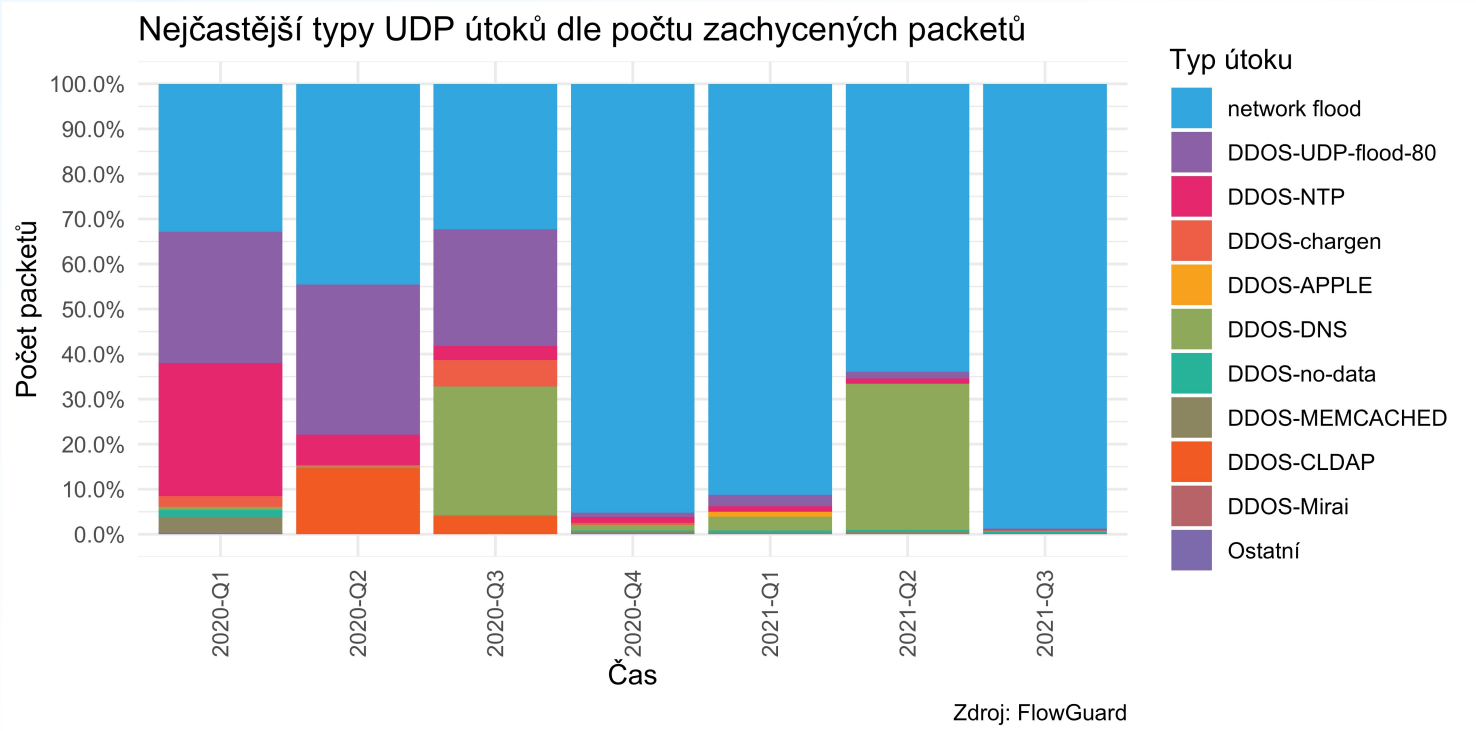
ComSource

Nejčastěji zneužívané protokoly



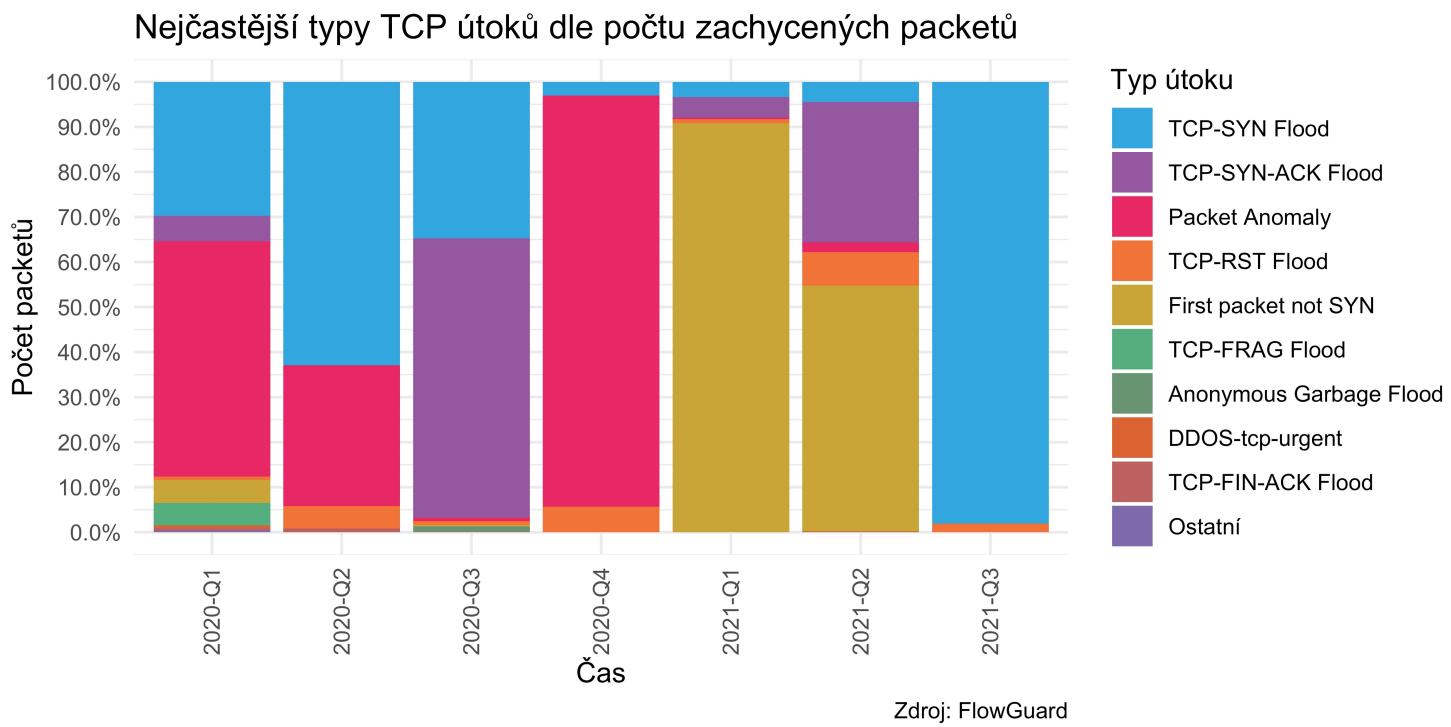
Com Source

Trend používaných útoků pro UDP



Com Source

Trend používaných útoků pro TCP

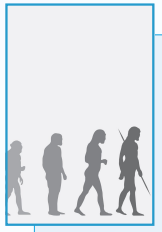


ComSource

Závěrečné shrnutí

Intenzita útoků roste

- Běžně přes 200 Gbps
- Je třeba se předem definovat threshold obrana/obětování



Útoky se neustále vyvíjejí

- Motivy útoků následují společenské trendy a události
  - Politické zájmy
  - Ekonomické zájmy
  - Sportovní události

Každý může být cílem

- Pro útok stačí jen platební karta
- Útočit je možné na libovolný síťový prvek s IP adresou

Prevence a příprava

- Robustní infrastruktura
- Krizové scénáře a postupy
- Školení personálu
- Definice technických a ekonomických limitů obrany

Specializované služby ochrany

- FlowGuard Infrastructure Protection
  - On Demand
  - Always On
  - Hybrid

Com Source

Děkuji za pozornost

Email: petr.kadlec@comsource.cz

Tel: 774 744 725

ComSource