ComSource

# DDoS útoky a jak se na ně připravit

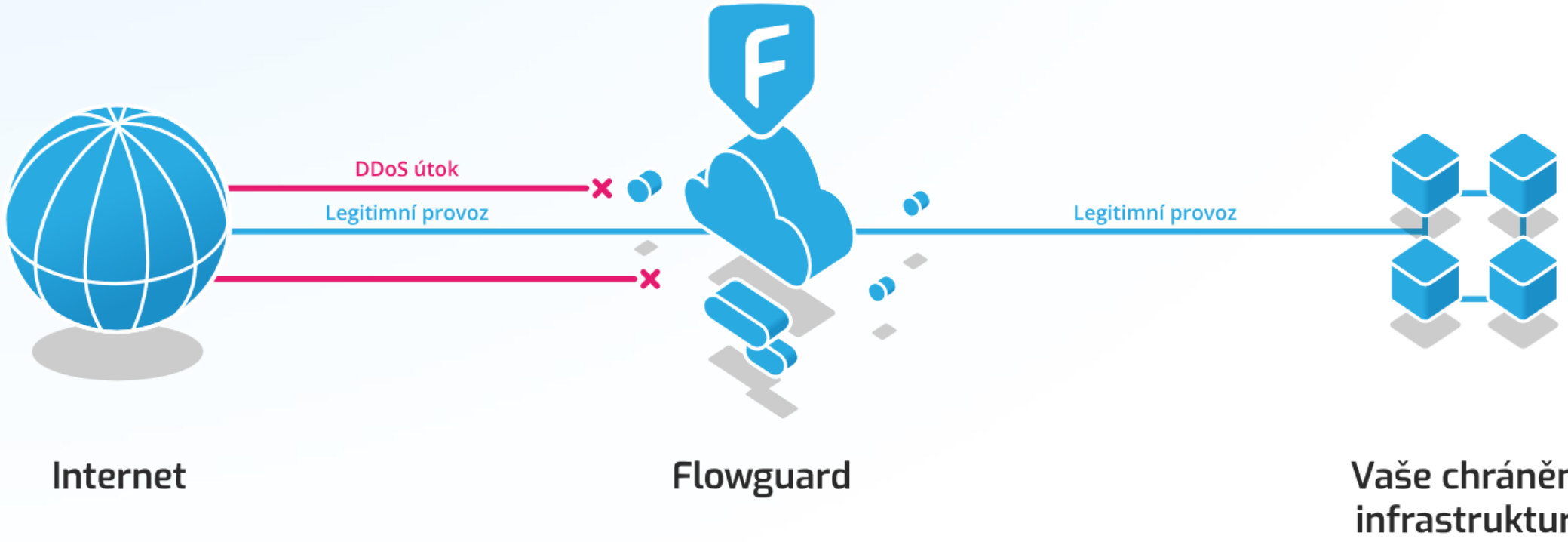
Petr Kadlec, ComSource s.r.o.

# Co je volumetrický útok?

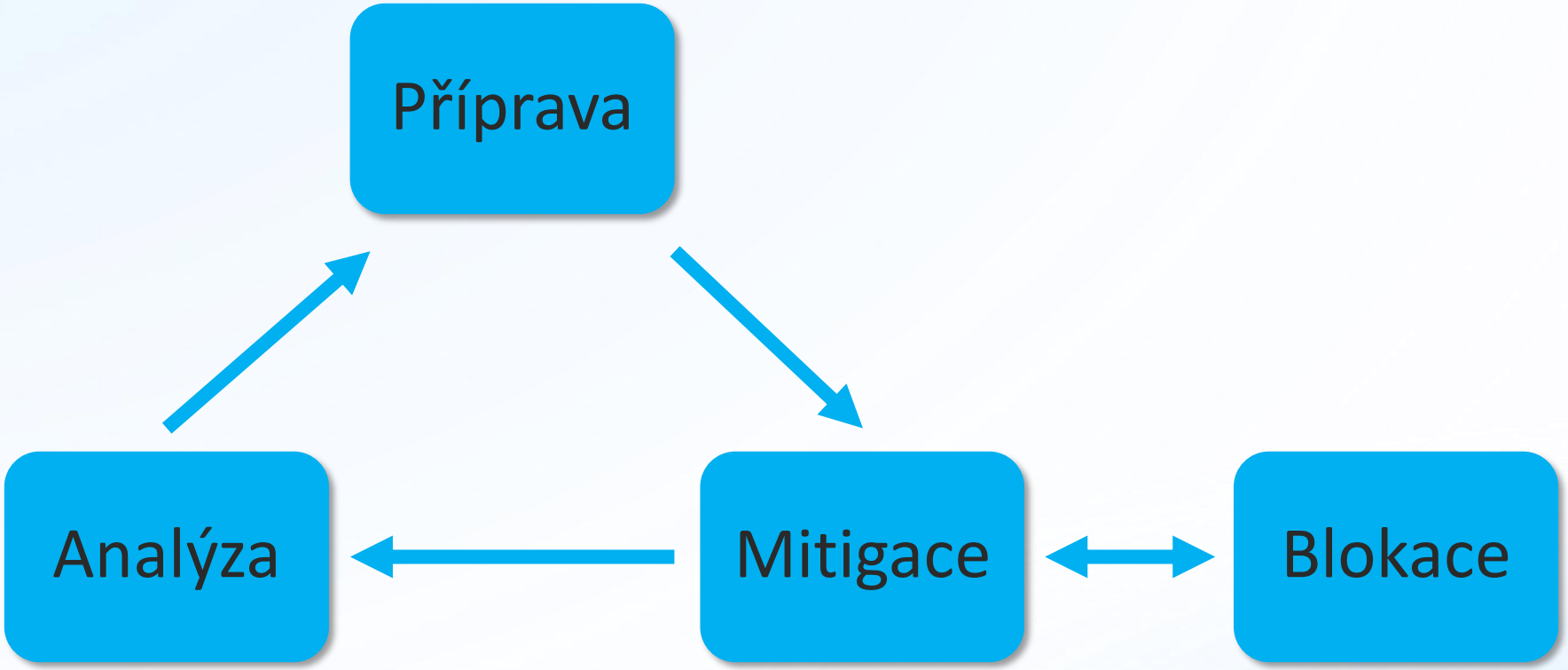
Průměrná cena DDoS útoku je cca 25 dolarů za hodinu.

| Princip | Motiv |
| --- | --- |
| • Abnormální síťový provoz<br>  • Na konkrétní službu či síťový prvek<br>  • Na celou infrastrukturu<br>• Negativní dopady<br>  • Vyčerpání systémových prostředků serverů<br>  • Vyčerpání systémových prostředků síťových prvků<br>  • Vyčerpání kapacity datových tras<br>  • Vyčerpání kapacity internetového připojení<br>• Výsledek<br>  • Nefunkční služba<br>  • Přetížená infrastruktura<br>  • Nedostupný internet | • Finanční zisk<br>  • Až zaplatíte přestaneme<br>  • Když nezaplatíte, budeme útok opakovat<br>• Nefunkční služby<br>  • Konkurenční boj<br>  • Politický boj<br>• Maskování jiné činnosti<br>  • Maskování chytrého útoku<br>  • Zaměstnání personálu<br>  • Vyřazení bezpečnostních a monitorovacích systémů přetížením<br>• Vandalismus |

# Princip ochrany



# Strategie obrany



# Příprava

| | |
|---|---|
| Robustní infrastruktura | • Výkon a datová propustnost<br>• Viditelnost provozu a monitoring<br>• Redundance |
| Minimální terč | • Limitace přístupu na všechny IP adresy bez aplikačních služeb<br>• Limitace systémových prostředků<br>• Blokace nepoužívaných služeb |
| Nástroje pro mitigaci a blokaci | • Definice ekonomických a technických limitů pro rozhodování<br>• AntiDDoS ochrana<br>• RTBH/Flowspec |
| Krizové plány a postupy | • Postupy pro detekci a reakci na útok<br>• Plány na omezení provozu (podmíněná limitace provozu, GeoIP)<br>• Plány ostrovního provozu/FENIX |

# Mitigace

**Mitigace L4 útoků**

- Hrubé síto
- Co nejblíže do internetu (cloud)
- Přesměrování trvalé/v případě potřeby

**Mitigace L7 útoků**

- Jemné síto
- Co nejblíže u chráněné služby (perimetr)
- Obvykle integrace s NGFW, ADC/WAF

**Sběr dat**

- Metadata o síťovém provozu
- PPS/BPS/RPS časové řady
- Data z L4 a L7 mitigace

# Blokace

| | |
|---|---|
| Rutinní postupy pro spuštění blokace | • Kritéria pro aktivaci blokace<br>• Detekce blokované adresy/protokolu<br>• Blokace jen na nezbytných trasách |
| Blokace (RTBH, Flowspec) | • Blokace ve vlastní síti (ASBR)<br>• Export informace dodavatelům konektivity<br>• Oznámení blokovanému subjektu |
| Testování konce útoku | • Monitoring průvodních jevů<br>• Testovací pozastavení blokace |

# Analýza

**Vyhodnocení útoku**

- Identifikace jednotlivých vektorů útoku
- Identifikace cílů útoku
- Vyhodnocení úspěšnosti útoku

**Vyhodnocení obrany**

- Dopad na napadenou službu
- Dopad na ostatní služby
- Dopad na síťovou infrastrukturu

**Definice a implementace opatření**

- Optimalizace limitů
- Optimalizace postupů
- Implementace optimalizací a testování

# Opravdu vás ISP ochrání?

**Kontrolní otázky na ISP**

- Do jaké intenzity či délky trvání útoku jsme chráněni?
- Jak funguje monitoring/reporting útoků?
- Jaké máme SLA na mitigaci útoků?
- Kolik za ochranu platíme?

## Zájmy ISP

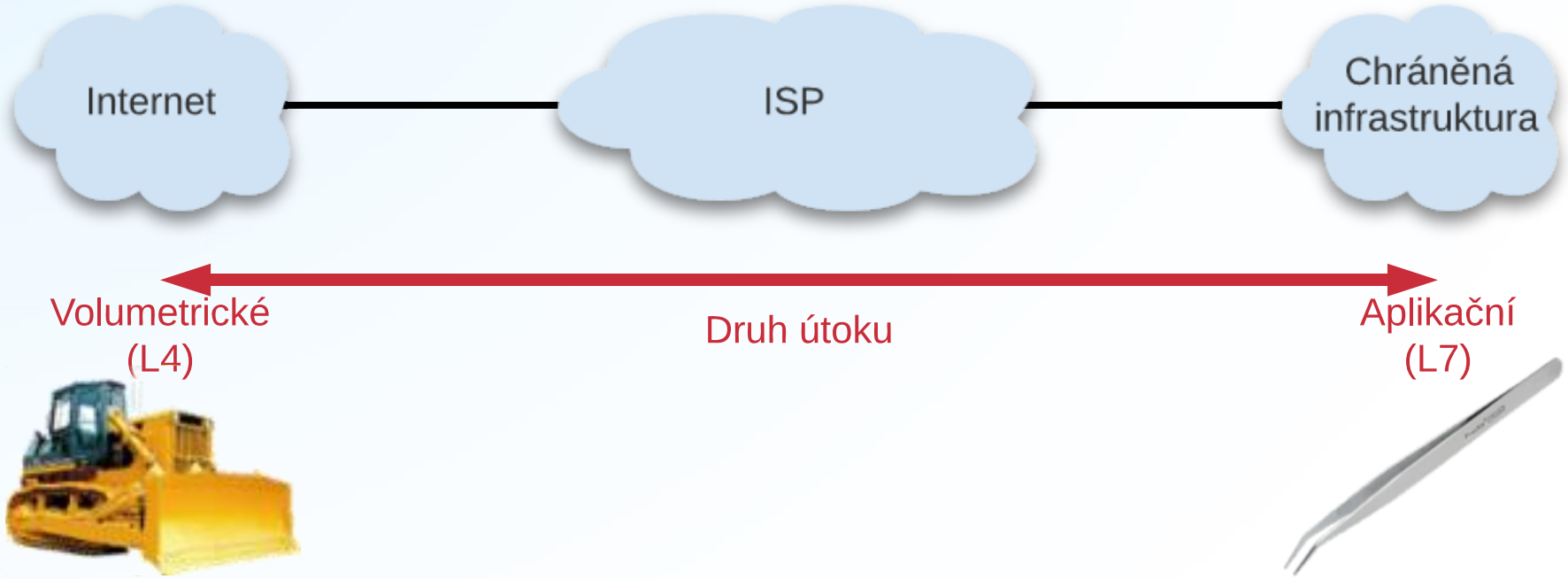
- Atraktivní služby pro zákazníky
- Maximální využití investic do infrastr.
- Ochrana vlastní infrastruktury (jeden vs. mnoho zákazníků)
- Zisk z konektivity
- Zisk z pronájmu tras

## Zájmy zákazníka

- Dostupnost a kvalita připojení
- Nízké náklady

Com Source

# Nejvhodnější místo pro mitigaci útoků

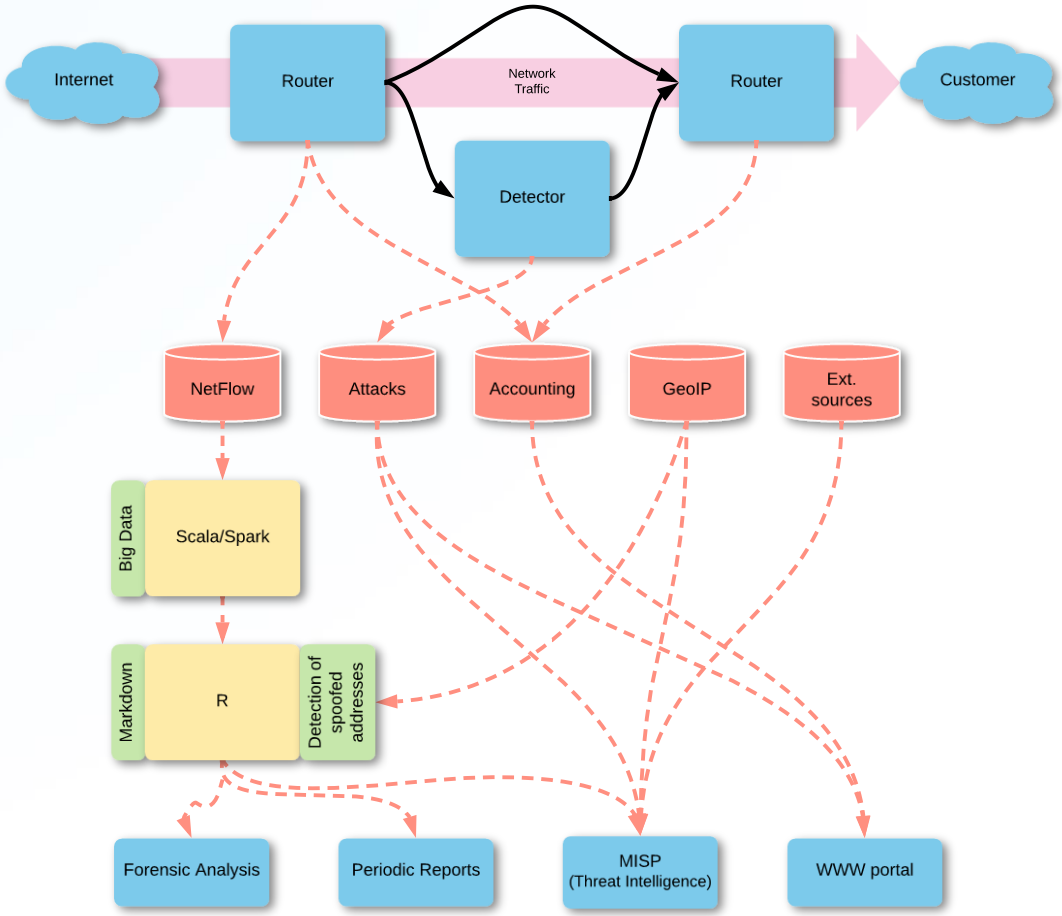



- Hrubá filtrace
- Může ohrozit infrastrukturu
- Transparentní pro legitimní provoz

- Jemná filtrace
- Neohrožuje infrastrukturu
- Nutno terminovat a dešifrovat síťový provoz

# Data, data, data…

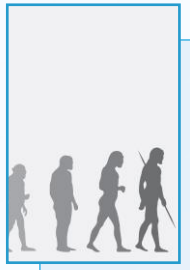
- Sběr a zpracování informacích o útocích
- Popis vektorů útoku
- Zjišťování zdrojových IP adres
- Reputační databáze
  - Seznamy IP, ASn a subnetů dle zdroje pořízení
  - Časová informace pořízení
  - Poločas rozpadu (platnosti)
- Výstupy
  - Forenzní analýzy a reporty
  - Threat Intelligence/MISP
  - WWW portál



# Shrnutí problematiky útoků

## 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

Com Source