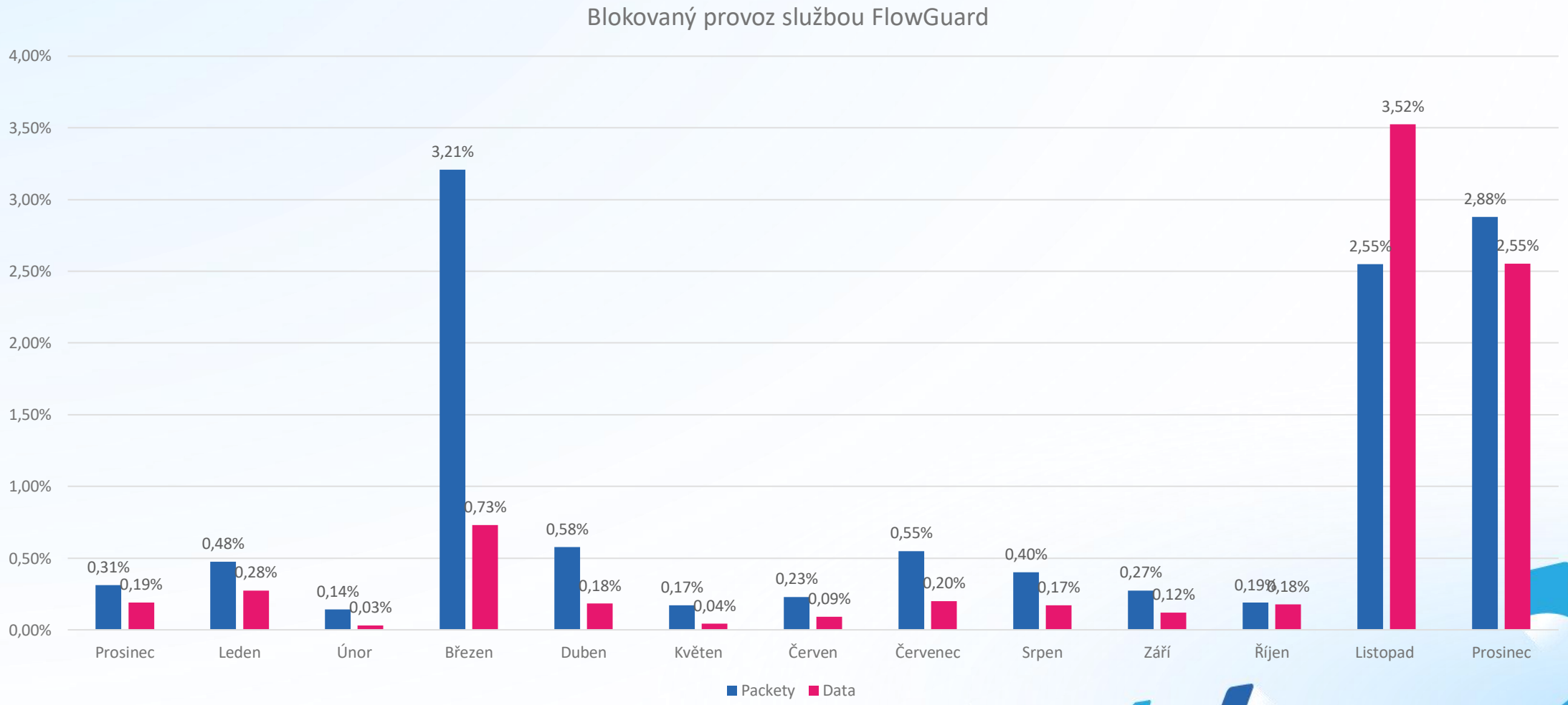
ComSource

Novinky a trendy v DDoS

Petr Kadlec, ComSource s.r.o.

Trend intenzity útoků

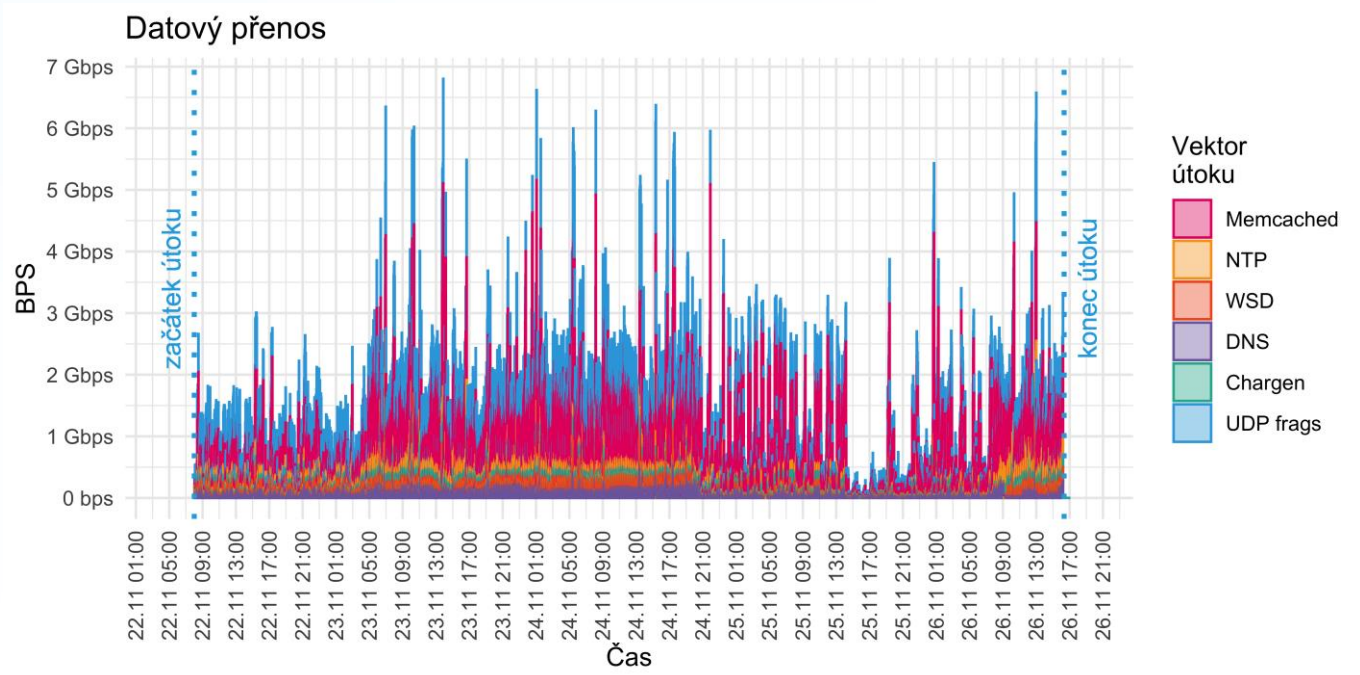


Com Source

Dlouhé útoky

- Doba trvání útoků bývá jednotky či desítky minut
- Delší útoky jsou vzácné, obvykle za nimi stojí nějaká kampaň a mají menší intenzitu (jsou pod rozlišovací schopností transitních operátorů)
- Konektivita se obvykle účtuje metodou 95th percentilu
- 5% měsíčního času je cca 1,4 – 1,55 dne
- RTBH vs. neočekávané náklady

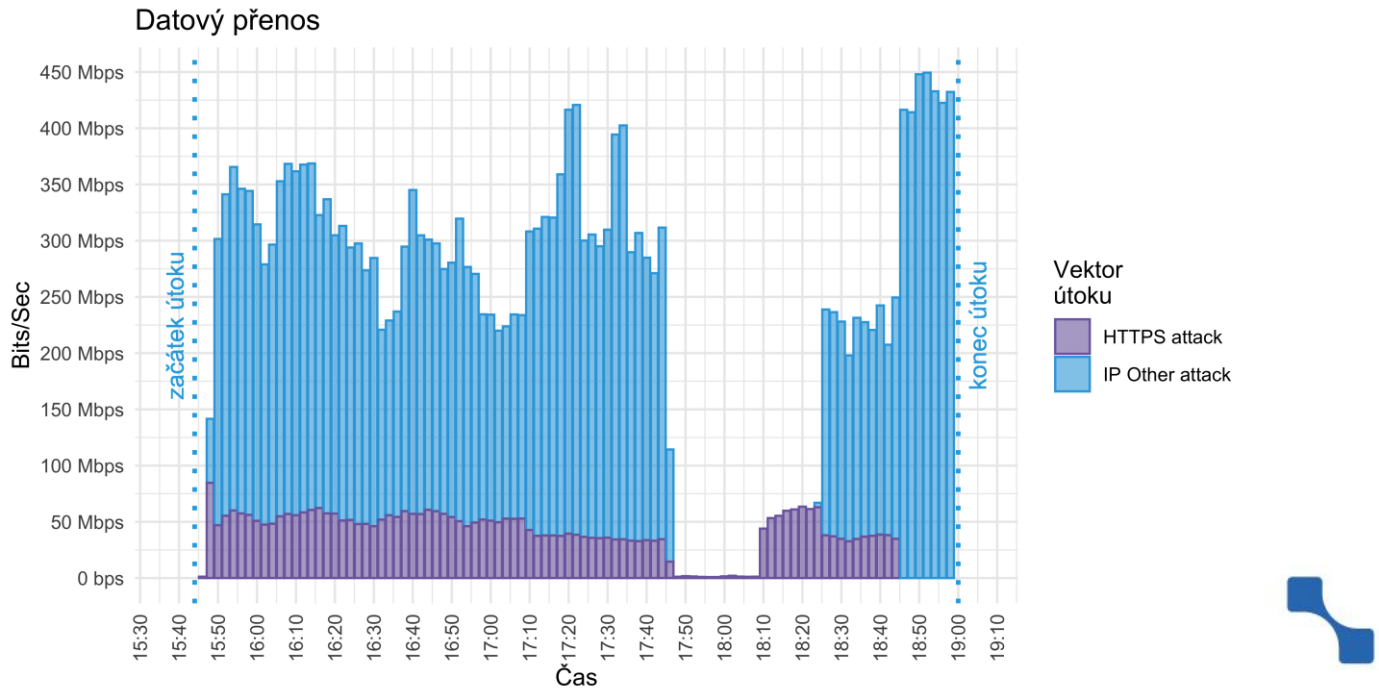
ID	Protokol	Src Port	Dst Port	Popis
Memcached	UDP	11211	3306	Memcached amplification attack
NTP	UDP	123	3306	NTP amplification attack
WSD	UDP	3702	3306	WS-Discovery amplification attack
DNS	UDP	53	3306, 80	DNS amplification attack
Chargen	UDP	19	3306	Chargen amplification attack
UDP frags	UDP	0	0	UDP fragments



Exotické IP protokoly

- Troubleshooting
  - Chybějící znalosti a zkušenosti
- Monitoring a měření
  - Countery vs. metadata
  - Dashboardy
- Neočekávaný průnik
- Neočekávané chování síťových prvků
- Jsou opravdu třeba?
  - Blokace na hranici sítě/AS
  - Blokace na bezpečnostním perimetru

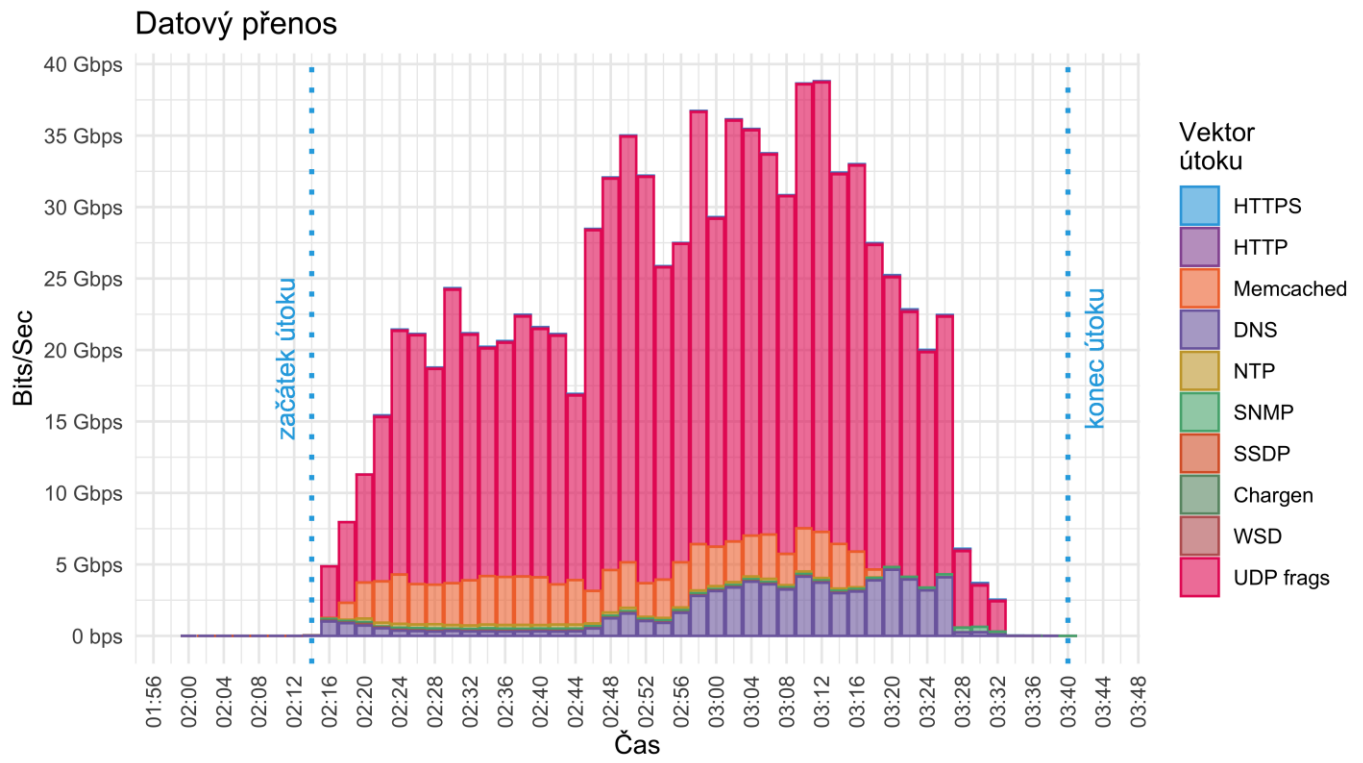
ID	Protokol	Popis
HTTPS attack	TCP	Flood na HTTPS z podvržených adres
IP Other attack	UTI, TRUNK-2, IPv6-ICMP, LARP, Mobility-Header, TCF, FC, SNP, IPv6, MOBILE, MERIT-INP, LEAF-2, PIPE, CPHB, SM, NARP, VISA, CRTP, SUN-ND, BBN-RCC-MON, ARGUS, WSN, SKIP, EGP, IDPR, NETBLT, 99, IPX-in-IP, GGP, Shim6, HIP, EMCON, UDPLite, TLSP, RVD, LEAF-1, IDPR-CMTP, EIGRP, IPComp, ENCAP, 61, CBT, VRRP, AX.25, IPv6-NoNxt, VMTP, STP, DCCP, Compaq-Peer, DCN-MEAS, RDP, XNET, SRP, SWIPE, I-NLSP, VINES, TTP, IL, IPv6-Route, TRUNK-1, 68, DDP, ISO-TP4, SAT-MON, PVP, SCPS, BNA, CRUDP, MUX, TP++, MTP, SMP, 144, NSFNET-IGP, DGP, MFE-NSP, SSCOPMCE, CPNX, PGM, 3PC, WB-MON, 114, IPv6-Frag, WESP, IRTP, IPIP, ISIS, ETHERIP, CHAOS, HMP, 143, IPCV, SECURE-VMTP, manet, Sprite-RPC, ESP, IDRP, PNNI, XTP, PUP, DDX, PRM, SPS, WB-EXPAK, ARIS, PIM, AH, 63, X...	Flood na všechny ostatní IP protokoly z podvržených adres



Kobercové nálety

- Cílem je mnoho adres nebo celý subnet
- Obvykle kombinuje více typů útoků a protokolů
- Problematické RTBH
  - Velikost prefixu /32
  - Omezený počet prefixů
- Doporučení
  - Rozšíření RTBH
  - Flowspec

ID	Protokol	Src Port	Dst IP	Popis
HTTPS	TCP	443	x.x.x.x/24	HTTPS flood z podvržených IP adres
HTTP	TCP	80	x.x.x.x/24	HTTP flood z podvržených IP adres
Memcached	UDP	11211	x.x.x.x/24	Memchached amplification attack
DNS	UDP	53	x.x.x.x/24	DNS amplification attack
NTP	UDP	123	x.x.x.x/24	NTP amplification attack
SNMP	UDP	161	x.x.x.x/24	SNMP amplification attack
SSDP	UDP	1900	x.x.x.x/24	SSDP amplification attack
Chargen	UDP	19	x.x.x.x/24	Chargen amplification attack
WSD	UDP	3702	x.x.x.x/24	WSD amplification attack
UDP frags	UDP	0	x.x.x.x/24	UDP fragments



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 automatizace pro změny konfigurace síťových prvků
- Definice stupňů obrany a automatické přecházení mezi nimi

Děkuji za pozornost

Email: petr.kadlec@comsource.cz

Tel: 774 744 725

ComSource