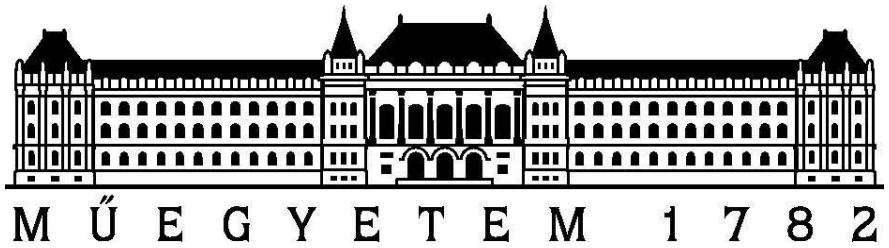
DDOS VÉDELEM

NAGY BALÁZS

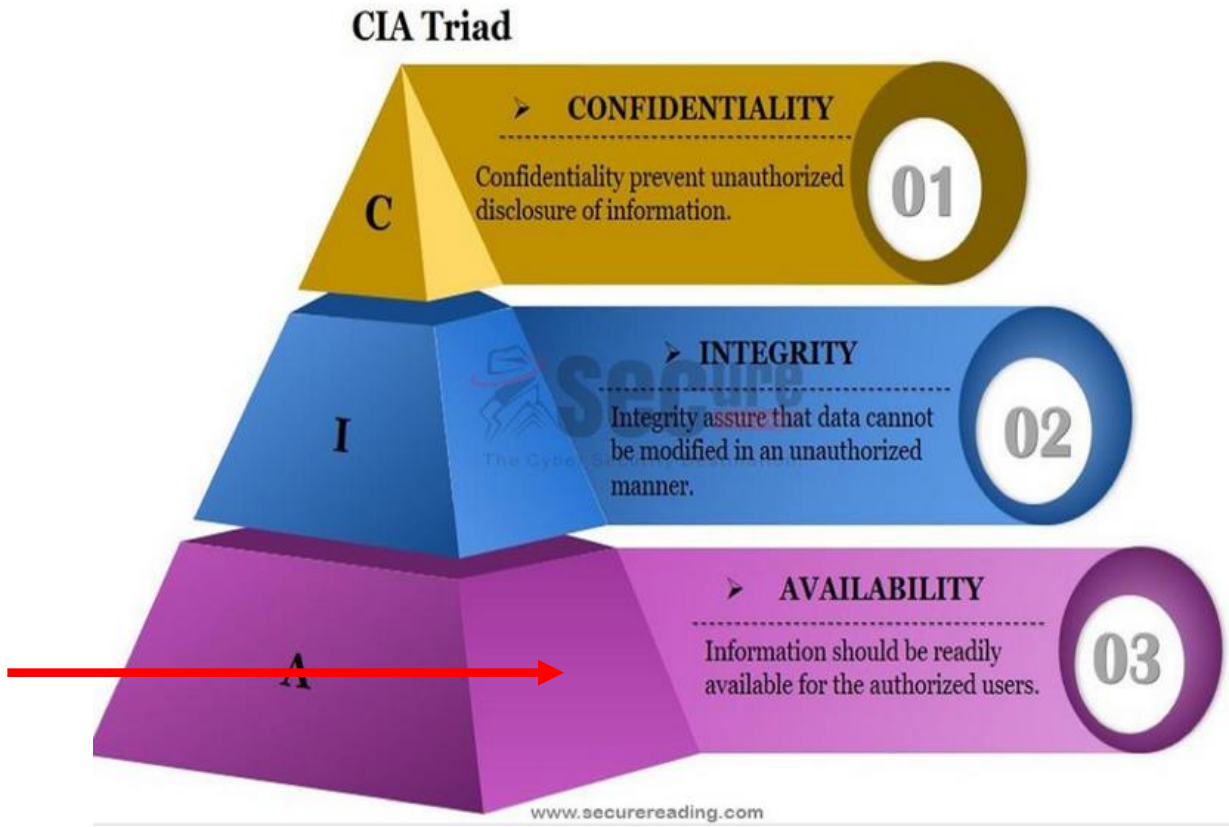


SmartComLab

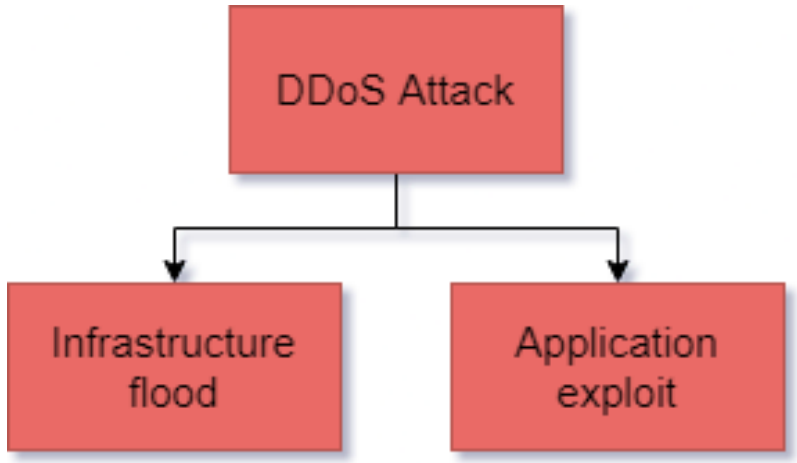
AITIA

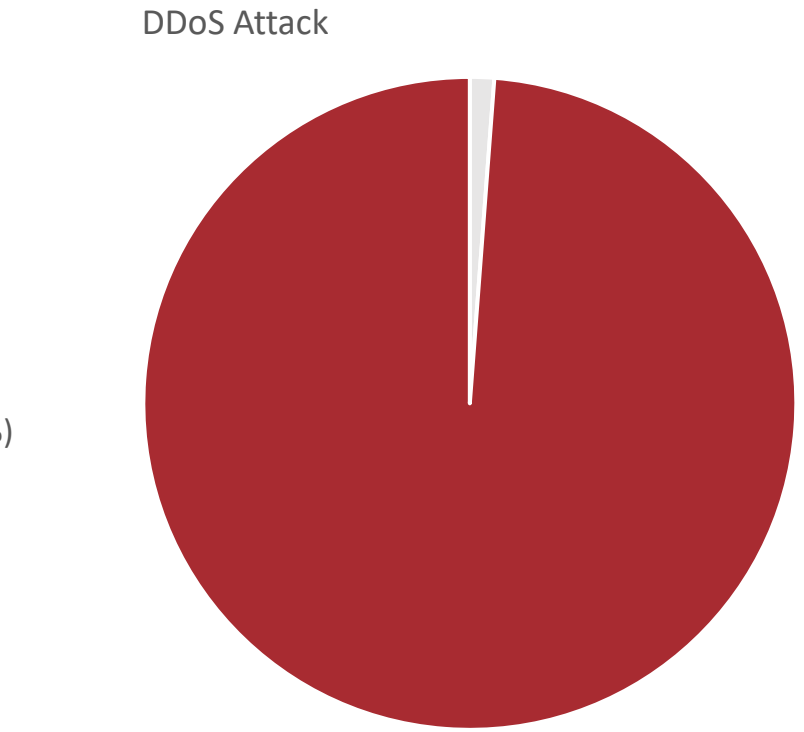
DDoS (Distributed Denial of Service)

- Internetes infrastruktúra túlterhelése, használhatatlanná tétele
- Elárasztás nagy mennyiségű IP csomaggal
- 4. generációs hadviselés
- Olcsó kiforott technológia



DDoS FŐ FAJTÁI





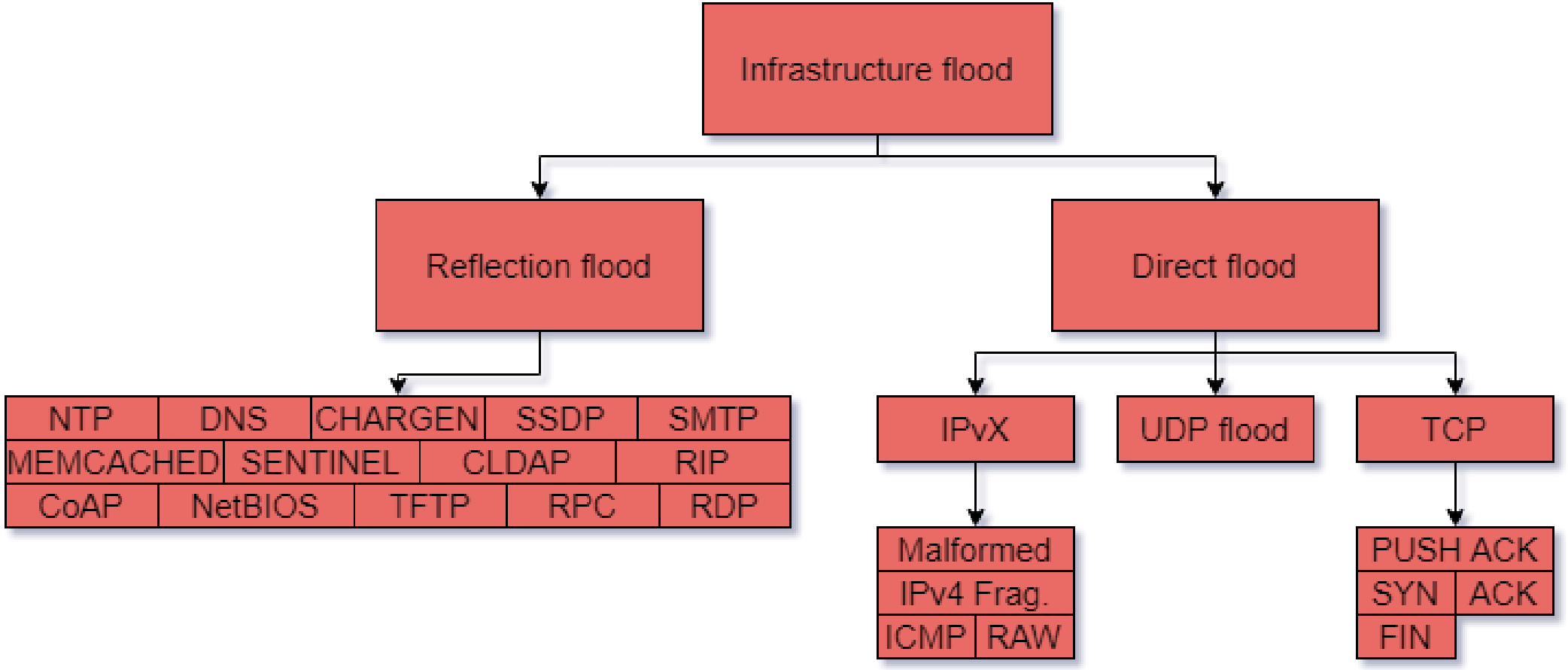
Applikációs DDoS

- Adott protokoll vagy szoftver gyengeségének kihasználása
- Nagyon sok fajta támadás fajta létezik
- Nagyon komoly károkat tud okozni
- Mégis ritka, mert komoly protokoll/szoftver ismeret szükséges hozzá
- Leggyakoribbak a HTTP alapú támadások (pl. HTTP get)
- Védekezni az adott applikáció tud a leghatékonyabban ellene
- Tipikus védelmek: Captcha, WAF, sw update

Infrastruktúra túlterheléses DDoS

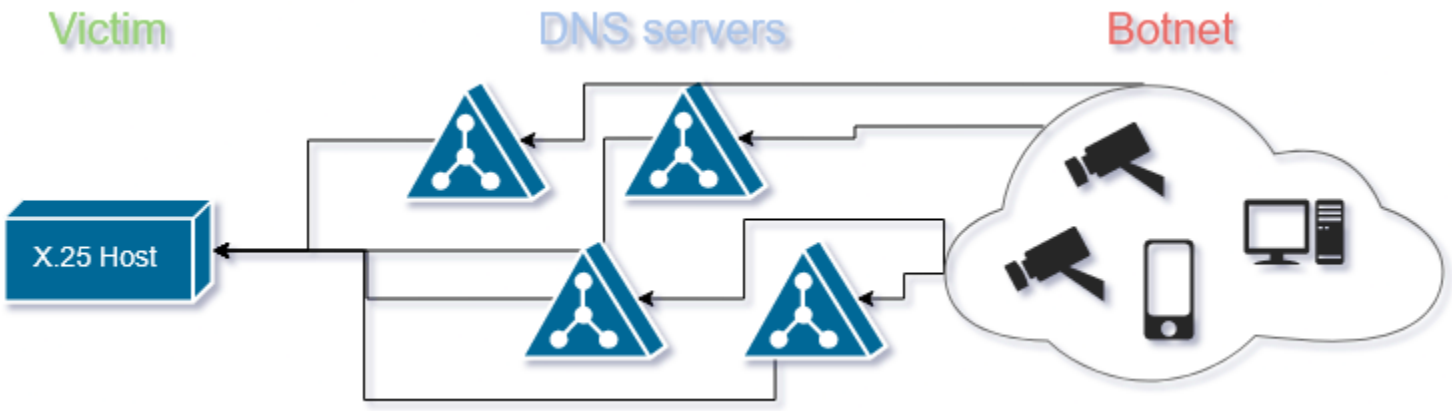
- Hálózat vagy szerver erőforrásainak kimerítése
- 100-nál kevesebb támadás fajta, implementációban jelentős különbségek
- Elérhetetlenné tudja tenni vagy a QoS-t lerontja
- Nagyon gyakori, mert semmi fajta informatikai túdást nem igényel
- Védekezni ISP szinten a leghatékonyabb
- Tipikus védelmek: DDoS tüzfal, Cloud service-k

INFRASTRÚKTÚRA DDOS TÁMADÁSOK LEBONTÁSA



REFLEKTÁLT ELÁRASZTÁS

- Az interneten elérhető szolgáltatások (DNS,NTP,CLDAP, stb.) felhasználása támadás megerősítésére és anonimizálására
- Spoofolt source IP-vel adnak fel lekérdezéseket

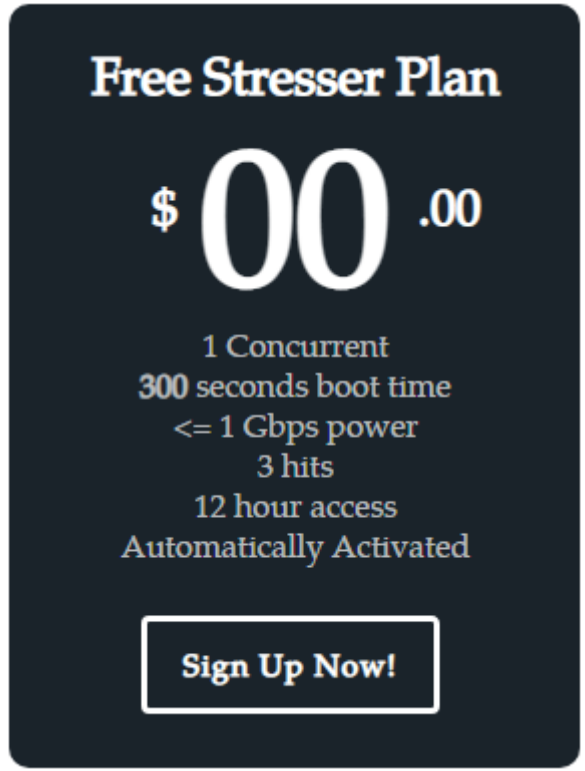


DIREKT ELÁRASZTÁS

- A támadó direktben célozza meg az áldozatot
- Jellemzően UDP, TCP is előfordul
- Nagyon szofisztikált is lehet, pl. előre felvett nagy sávszélességű multimédiás forgalom visszajátsása
- Potenciálisan ezeket a legnehezebb felismerni

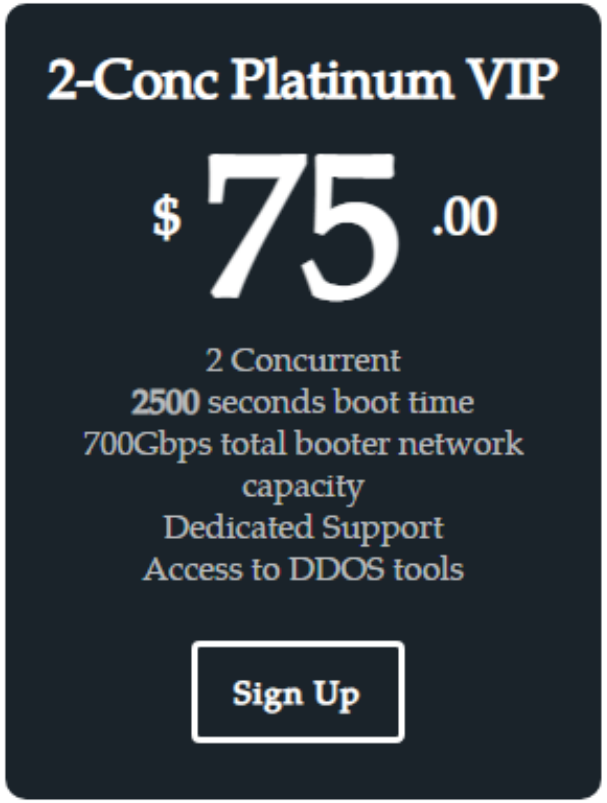
Hogyan készül a DDoS

- 2021-ben a DDoS-ok forrása majdnem kizárólag automatizált botnetek
- A botnetekhez hozzáférést lehet venni
- A DDoS szolgáltatások teljesen automatizáltak, a támadó csak kiválasztja a támadás formáját és a célt
- Gyakorlatilag visszakövethetetlen ki indította a szolgáltatást
- Több DDoS szolgáltató ingyenes próba verziót is biztosít



DDoS TÁMADÁS MENETE

- DDoS szolgáltatás kiválasztása TOR böngésző segítségével
- Monero vagy más visszakövethetetlen kríptóvaluta vásárlása kríptó váltónál
- Monero áthelyezése privát tárcába
- Monero átutalása a Botnet üzemeltetőjének
- Cél IP kiválasztása
- Támadás



DDoS TÁMADÁSOK JELENTŐSÉGE

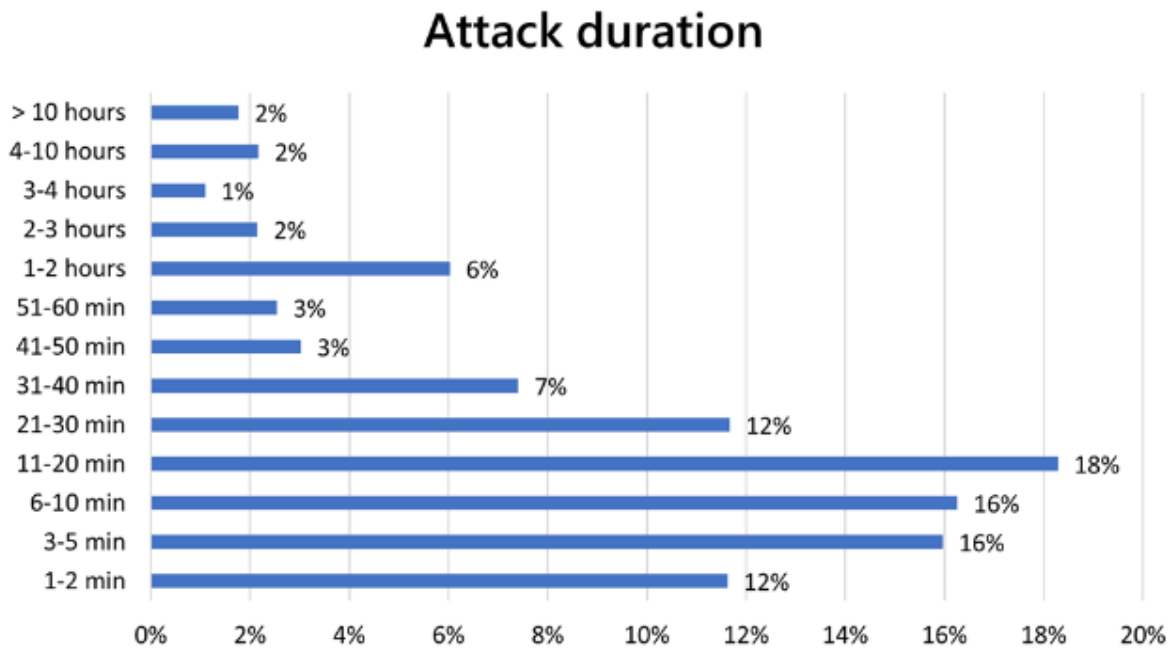
- Nagyon sok van, az AITIA által monitorozott hálózatokban minden naposak a jelentős támadások
- Támadások 99%+ -a külföldről származik
- Majdnem minden jelentősebb szolgáltatás ellen megpróbálkoznak: vakcina jelentkezés, előválasztás, nemzeti konzultáció
- Amit mi Magyarországon látunk az 5-7 évvel a nyugati szint mögött van, főleg sávszélességben
- Ennél már csak rosszabb lesz...

Elárasztásos DDoS védelem

- Átlagos felhasználó számára nem lehetséges az önálló védekezés
- Szolgáltatói oldalon a legjobb védekezni ellene, mivel a végfelhasználói internet sávszélességet nagyon könnyű telíteni
- Szolgáltatók számára sok megoldás áll rendelkezésre
- Legegyszerűbb megoldás, DDoS védett cloud szolgáltatások (Google, Amazon) használata, **de** ezzel minden adatunk elérhető lesz a szolgáltató számára

DDoS TRENDEK

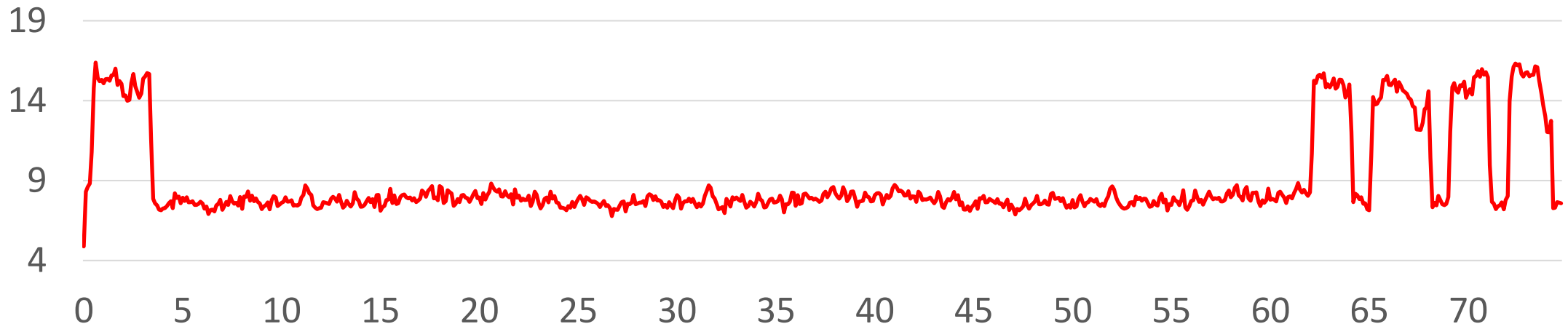
- A támadások hossza csökken
- A támadások gyakorisága növekszik
- A támadások szávszélessége növekszik
- A támadások kifinomultsága növekszik



Forrás: MS Azure DDoS Report 2021

HIT&RUN TÁMADÁSOK

- DDoS mitigáció általában manuális, lassú
- Legtöbb szolgáltató rendelkezik *valamilyen* DDoS védelmi megoldással
- Nincs értelme a támadásnak mitigáció után



AITIA SGA-NEDD

- Magyar fejlesztésű, Magyar tulajdonú DDoS védelmi rendszer
- Hardveres DDoS észlelés és szürés
- Támadások észlelése néhány ms alatt
- Intuitív, könnyen használható
- bnagy@aitia.ai

KÖSZÖNÖM A FIGYELMET!