EUROPEAN UNION AGENCY
FOR CYBERSECURITY

DDOS NAPADI IN ZAŠČITA

VSEBINA

Kaj je DDoS napad.

Vrste in primeri DDoS napadov.

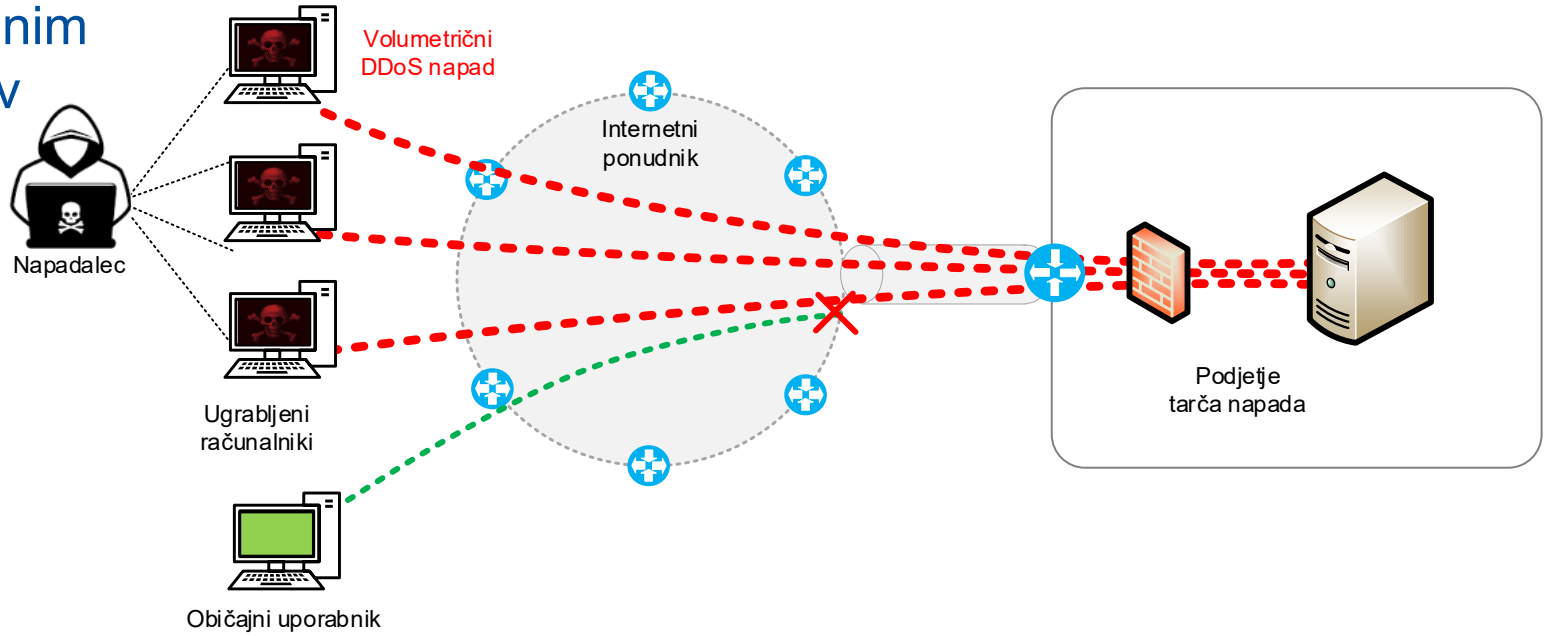
Učinki in posledice napadov.

Zaščita in odpornost pred DDoS napadi.

KAJ JE DDOS NAPAD

DDoS napad (Distributed Denial of Service) je vrsta kibernetskega napada, pri katerem napadalec preobremeni **strežnik, storitev ali omrežje** z ogromnim številom zahtevkov iz več različnih virov hkrati.

Cilj je onemogočiti normalno delovanje ciljane infrastrukture, tako da postane nedostopna za običajne uporabnike.



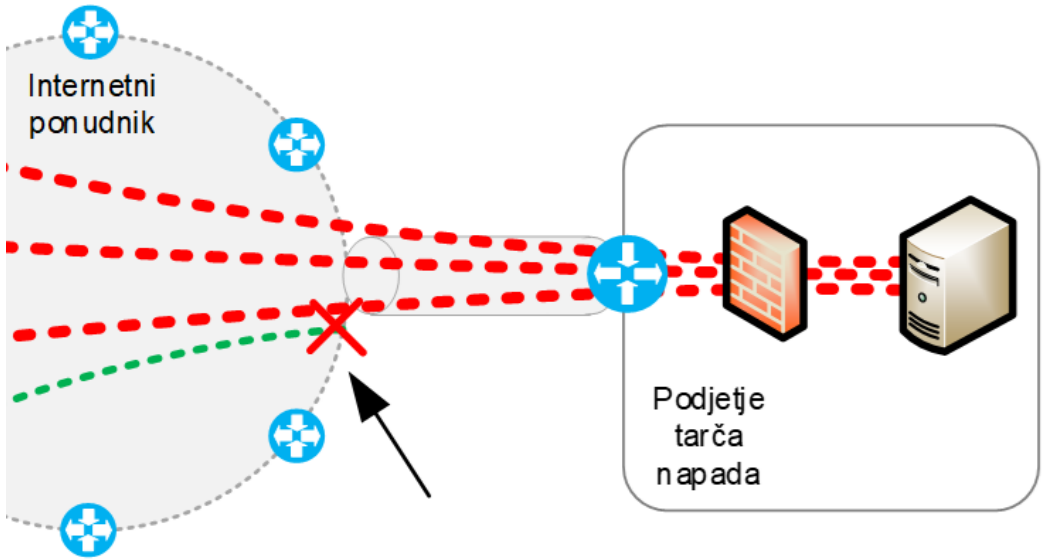
VRSTE DDOS NAPADOV

Volumetrični napadi

Poskušajo zapolniti pasovno širino do ciljnega omrežja storitve. Ti napadi so preprosto usmerjeni v povzročanje preobremenitve omrežja.

Napadalci pošljejo ogromno količino podatkov (merimo v Gb/s ali Tb/s) proti tarči, da zapolnijo njeno internetno povezavo. Posledica je, da se legitimni promet do storitve ne prebije skozi poplavo podatkov.

Tipični primeri so poplava UDP paketov (UDP flood), poplava ICMP (ICMP flood) ter reflektirani napadi z ojačitvijo (DNS amplification, NTP amplification, CLDAP ipd.), kjer majhne zahteve s strani hekerja sprožijo veliko količino prometa proti tarči.



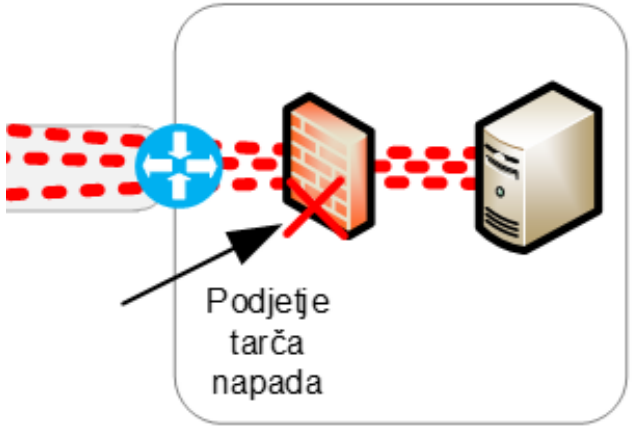
VRSTE DDOS NAPADOV

Protokolni napadi

Napadi na ravni omrežnih protokolov ciljajo na mehanizme komunikacijskih protokolov in omrežne naprave. Za napad ni nujno potrebna ogromna količina podatkov, namesto tega izrabljajo slabosti v protokolih ali preobremenijo strežnike z veliko količino omrežnih TCP zahtev.

Napadi izčrpavanja stanj TCP sej (TCP State-Exhaustion) ciljajo na zapolnitev tabele stanj TCP povezav (statefull), ki so prisotne v številnih omrežnih napravah, kot so delilniki bremena (load balancers), požarne pregrade (firewalls) in sami aplikacijski strežniki.

Pogosto uporabljeni napadi so: SYN flood, fragmentacijski napad, Ping of death, SSL Exhaustion, Smurf napad, DNS flood.



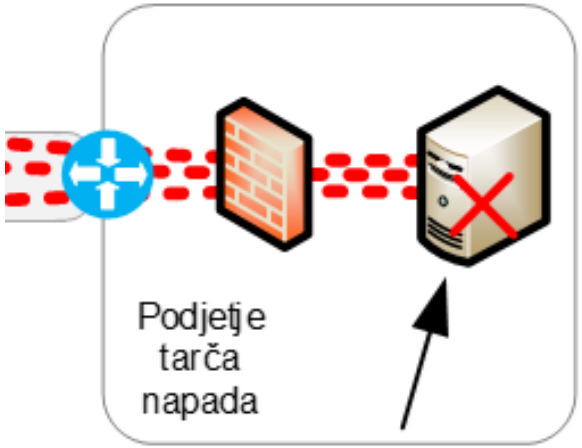
VRSTE DDOS NAPADOV

Aplikativni napadi

Napadi na aplikacijski sloj ciljajo določen vidik aplikacije ali storitve na 7. sloju (Layer-7). Napadi na aplikacijsko plast so postali med najpogostejšimi napadi onemogočanja storitev v zadnjih letih. Ti napadi so lahko zelo učinkoviti, ker je za onesposobitev strežnika dovolj majhna količina prometa, težćko pa jih je zaznati in proti njim učinkovito braniti.

Primeri aplikativnih napadov so: Slowloris, Slow POST, Slow READ, Low and Slow.

Današnji napredni napadalci združujejo volumetrične napade, napade izčrpavanja stanj in napade na aplikacijski sloj.



VRSTE DDOS NAPADOV

Aplikativni napadi

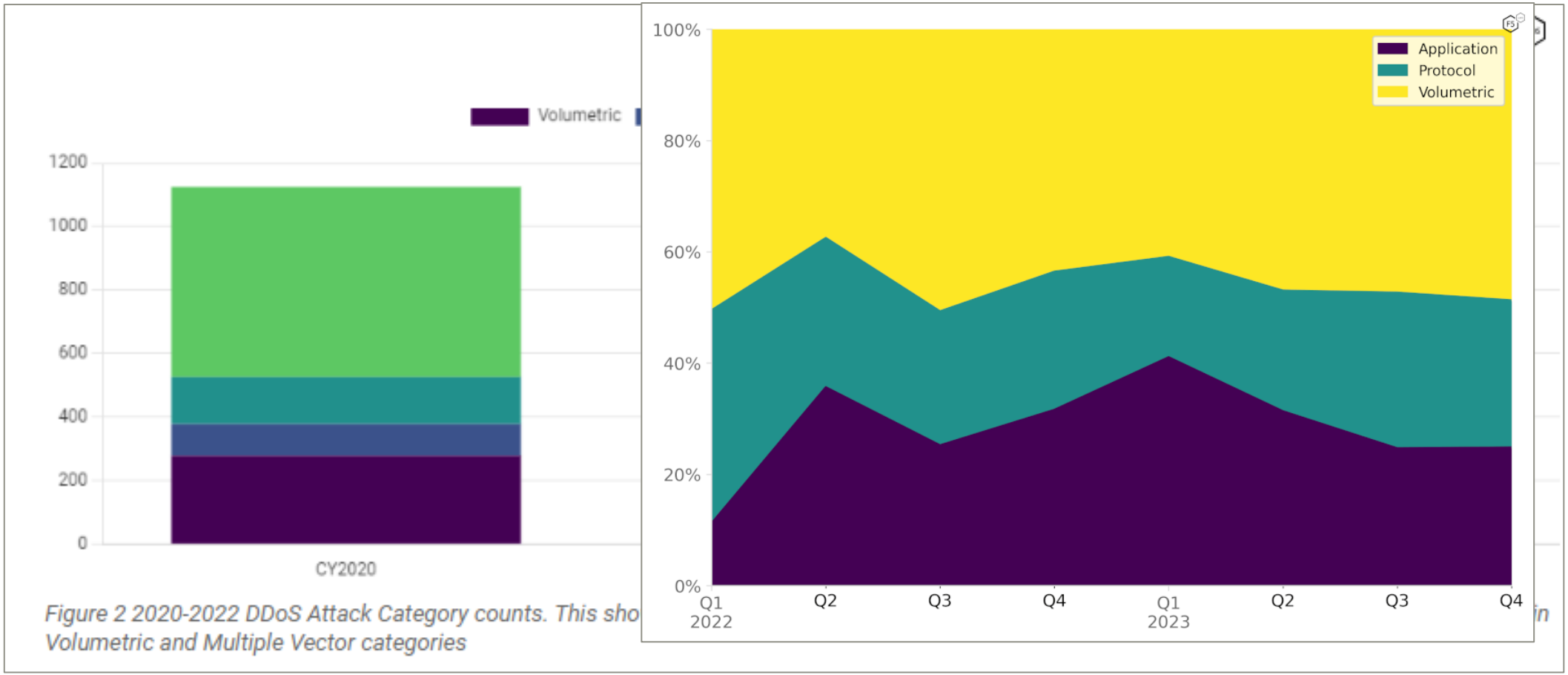


Figure 2 2020-2022 DDoS Attack Category counts. This sho ... in Volumetric and Multiple Vector categories

https://www.f5.com/labs/articles/2023-ddos-attack-trends

https://www.f5.com/labs/articles/2024-ddos-attack-trends

PODROBEN OPIS TEHNIK NAPADOV

DDoS Knowledge Base

All | Type keywords to search

DDoS General

117 Articles

- ICMP PING Flood
- SYN Flood
- ACK Flood
- FIN Flood
- URG Flood
- IP Fragmented...
- UDP Flood
- Empty Connection...
- ACK-PSH Flood
- ...more

SSL Attacks

4 Articles

- HTTPS Flood
- THC-SSL
- SSL Negotiation Flood
- HTTP/S Tor's Hammer

Layer 4

68 Articles

- ACK-FIN Flood
- URG-FIN Flood
- URG-PSH-FIN Flood
- URG-SYN Flood
- PSH Flood
- URG-ACK-RST-SYN-FI...
- URG-PSH Flood
- URG-PSH-SYN Flood
- PSH-SYN-FIN Flood
- ...more

HTTP Based attacks

33 Articles

- HTTP/S Cloudscraper...
- HTTP/S MHDDOS...
- HTTP/S MHDDOS GET
- HTTP/S Cloudscraper...
- HTTP/S Cloudscraper...
- HTTP PUT Flood
- HTTP/S MHDDOS CFB
- HTTP/S MHDDOS...
- HTTP/S Cloudscraper...
- ...more

Layer 7

44 Articles

- HTTP/S Cloudscraper...
- NTP Reflection Flood
- HTTP/S MHDDOS CFB
- HTTP/S MHDDOS...
- HTTP/S Cloudscraper...
- HTTP PUT Flood
- HTTP/S MHDDOS...
- HTTP/S MHDDOS GET
- HTTP/S Cloudscraper...
- ...more

Layer 3

4 Articles

- ICMP PING Flood
- ICMP Time Exceeded...
- IP Fragmented...
- ICMP Destination...

HTTPS Based attacks

33 Articles

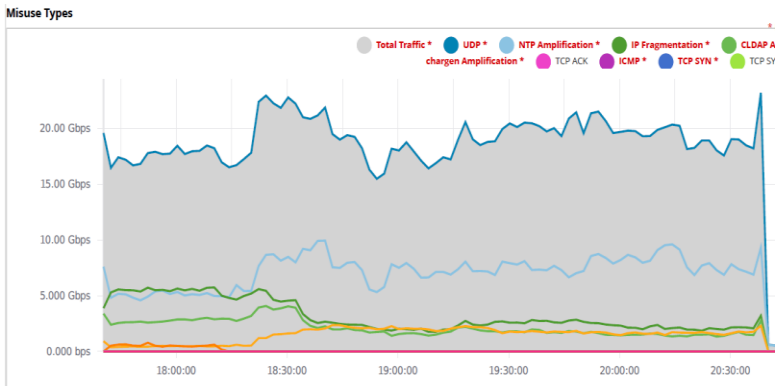
- HTTP/S Cloudscraper...
- HTTP/S MHDDOS...
- HTTP/S MHDDOS GET
- HTTP/S Cloudscraper...
- HTTP/S Cloudscraper...
- HTTP PUT Flood
- HTTP/S MHDDOS CFB
- HTTP/S MHDDOS...
- HTTP/S Cloudscraper...
- ...more

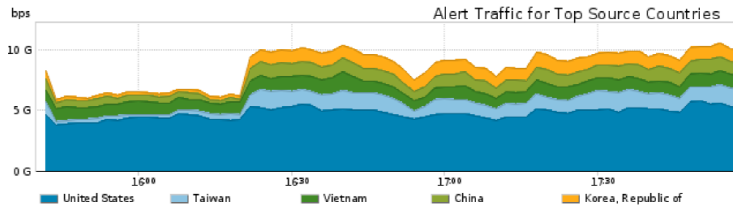
Vir: https://kb.mazebolt.com/

PRIMERI DDOS NAPADOV

Napad 1

Severity Level	Max Severity Percent	Top Misuse Type	Max Impact of Alert Traffic	Direction	Misuse Types
High	506,823.0% of 2 Mbps	NTP Amplification	25.4 Gbps/4.6 Mpps at Managed Object Boundary	Incoming	ICMP, IP Fragmentation, TCP SYN, Total Traffic, DNS, UDP, NTP Amplification, chargen Amplification, CLDAP Amplification



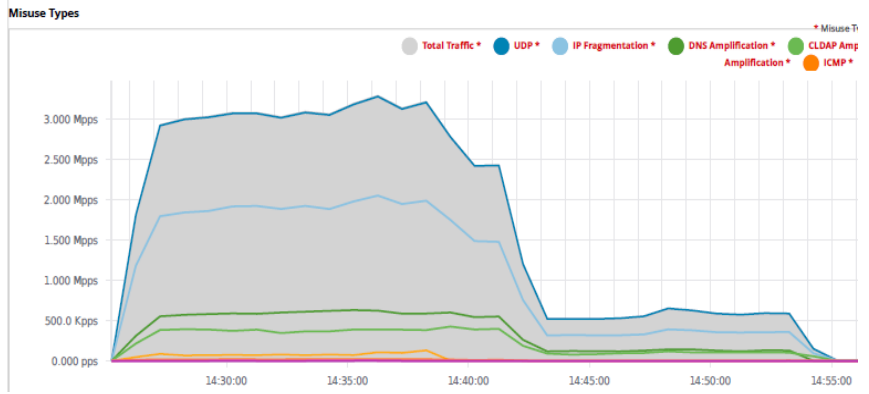


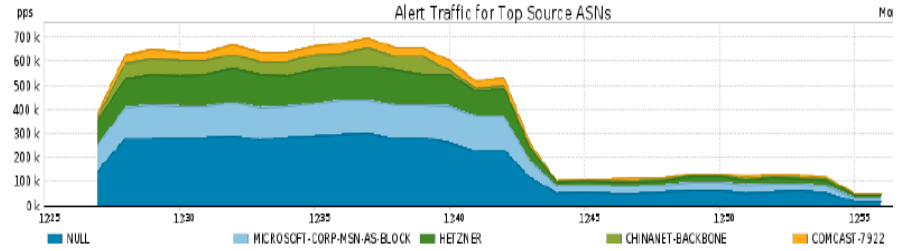
Source Countries

	United States	4.06 Gbps	25.15%
	Taiwan	900.20 Mbps	5.58%
	Vietnam	881.71 Mbps	5.47%
	China	796.29 Mbps	4.94%
	Korea, Republic of	742.82 Mbps	4.61%

Napad 2

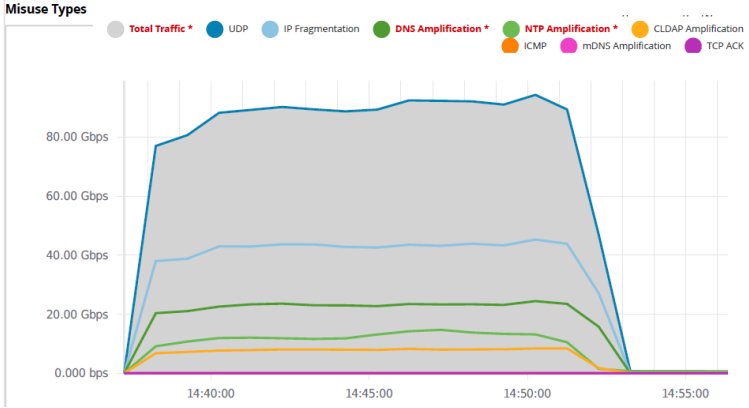
Severity Level	Max Severity Percent	Top Misuse Type	Max Impact of Alert Traffic	Direction	Misuse Types
High	134,030.0% of 5 Mbps	DNS Amplification	30.5 Gbps/3.3 Mpps at Managed Object Boundary	Incoming	ICMP, IP Fragmentation, Total Traffic, UDP, DNS Amplification, chargen Amplification, CLDAP Amplification

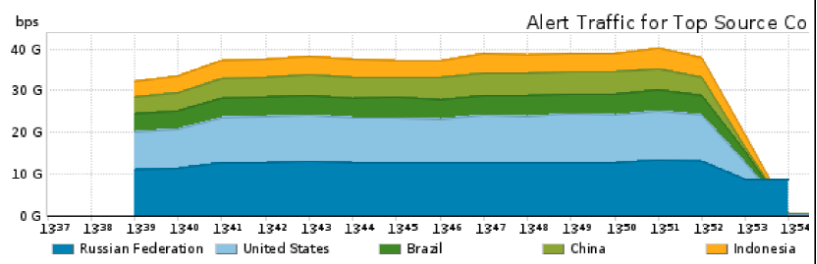




Napad 3

Severity Level	Max Severity Percent	Top Misuse Type	Max Impact of Alert Traffic	Direction	Misuse Types
High	14,479.0% of 200 Mbps	DNS Amplification	99.6 Gbps/11.9 Mpps at Managed Object Boundary	Incoming	Total Traffic, NT





DDOS NAPADI 2024

marec, april 2024

Russian Cyber Army , NoName057(16), HackNet

Together with our colleagues we sent DDoS missiles to 4 state websites in Slovenia 😈

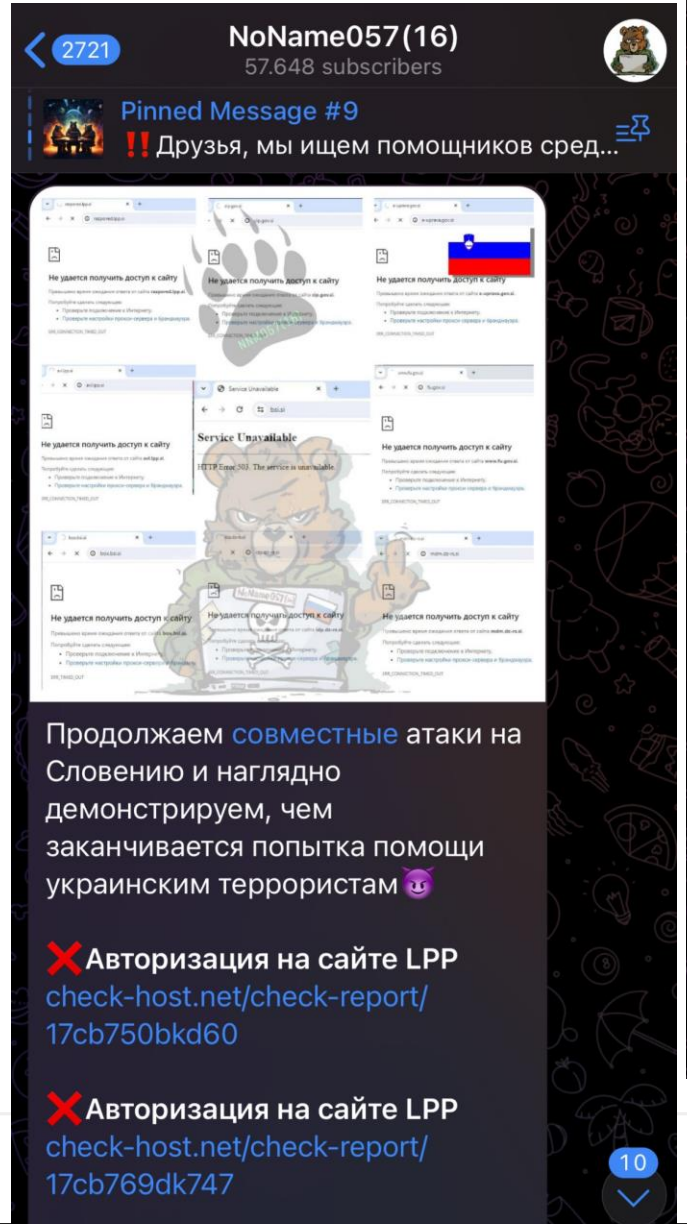
❌Statistical Office of the Republic of Slovenia
check-host.net/check-report/17cc98c2kd19
❌Ombudsman of the Republic of Slovenia (closed by geo)
check-host.net/check-report/17cc9bb8k69c
Subscribe ➡ NoName057(16)|DDoSia Project|Reserve|Eng version

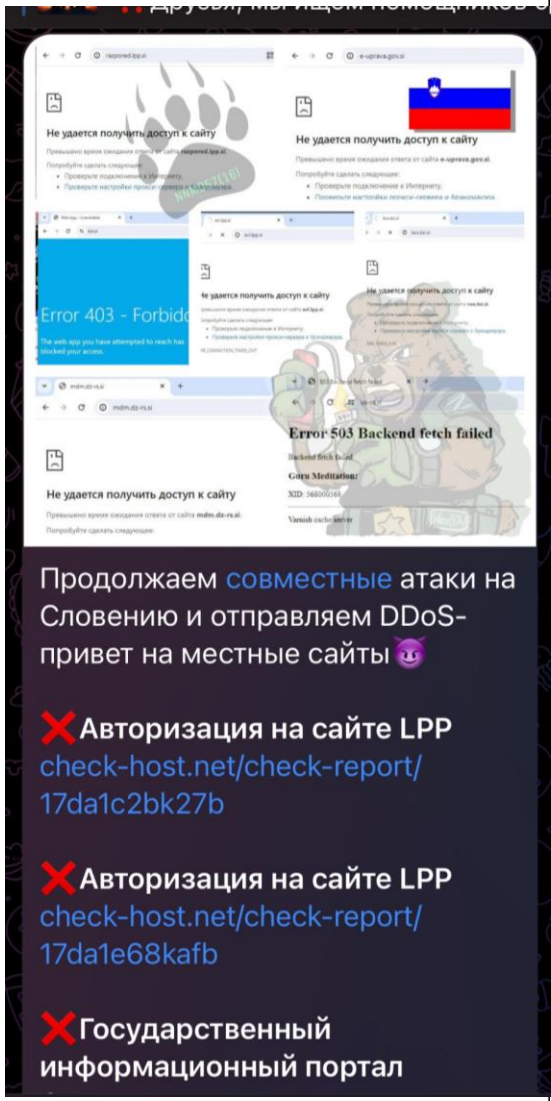
We continue our fascinating DDoS journey through the government websites of Slovenia 😈

❌State tax portal of Slovenia
check-host.net/check-report/17ea65b3k426
Subscribe ➡ NoName057(16)|DDoSia Project|Reserve|Eng version

We continue joint attacks on Slovenia and send DDoS greetings to local sites 😈

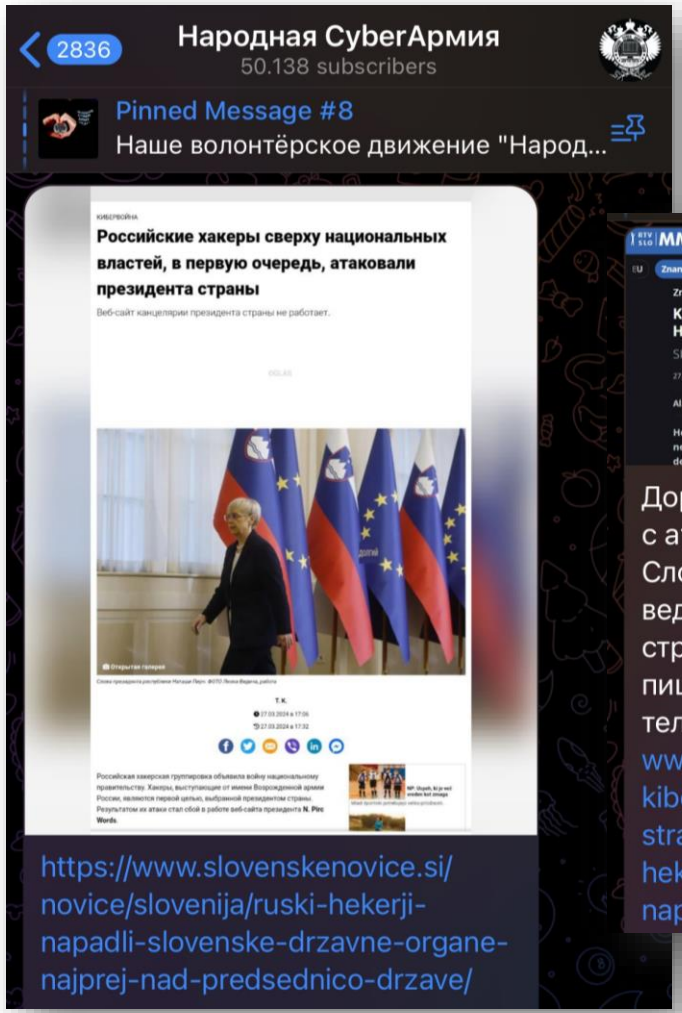
❌Authorization on the LPP website
check-host.net/check-report/17da1c2bk27b
Subscribe ➡ NoName057(16)|DDoSia Project|Reserve|Eng version

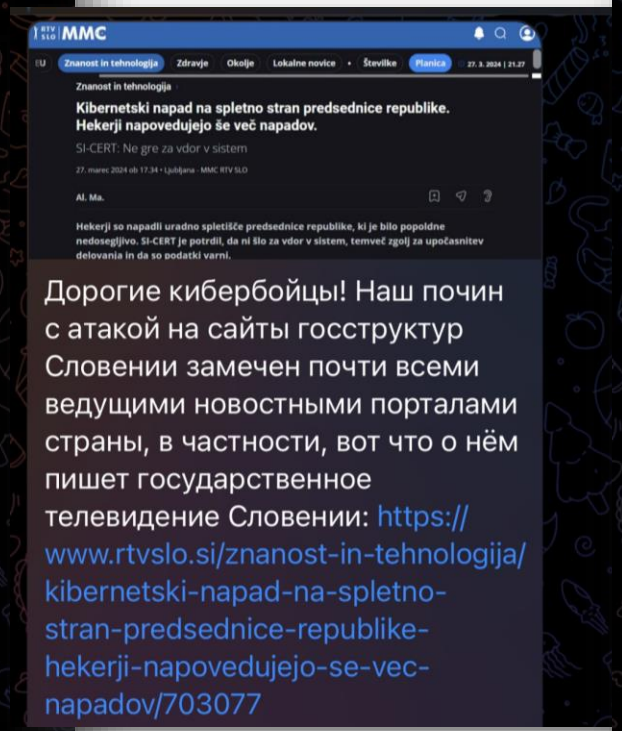


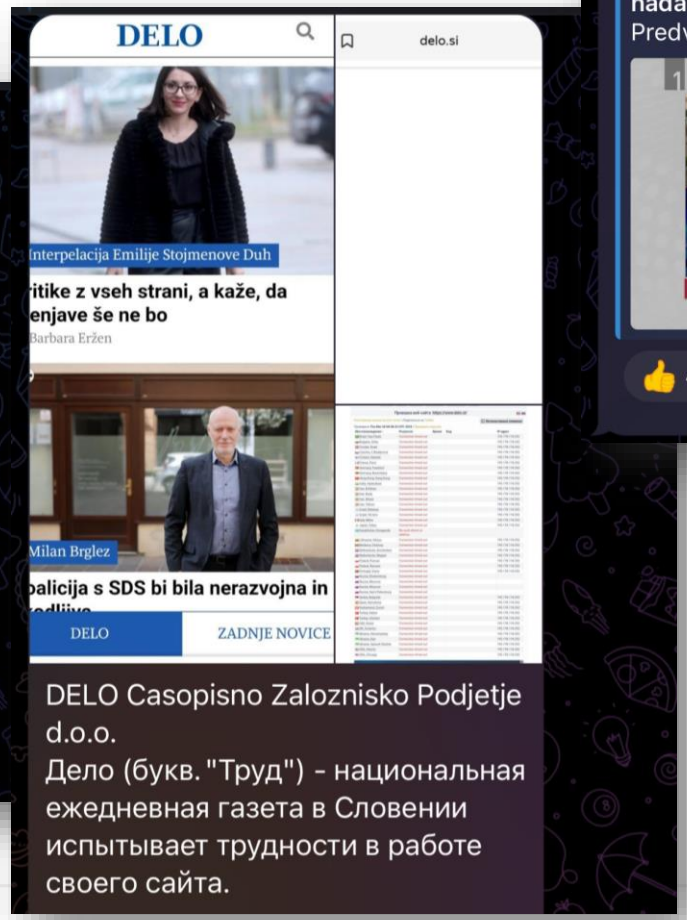


DDOS NAPADI 2024

Napadalci na Telegramu povzemajo slovenske medijske objave





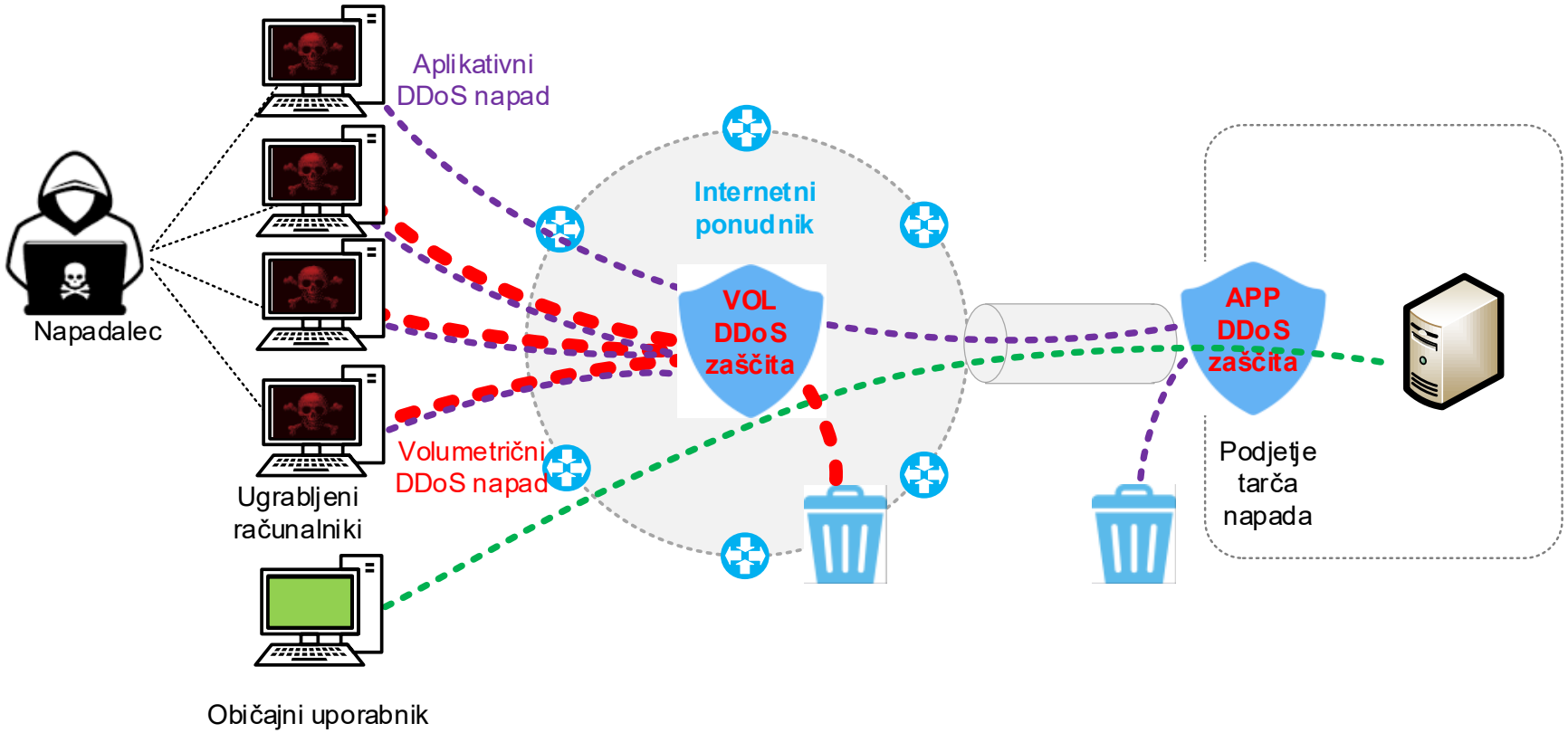


POSLEDICE DDOS NAPADOV

- **Izpad storitev**, spletne strani in spletne aplikacije niso dosegljive, tudi zunanje (v oblaku) storitve niso dosegljive za uporabnike podjetja.
- **Trajanje izpada** je lahko od nekaj minut do več ur ali celo dni pri ponavljajočih napadih.
- **Škoda** je odvisna od tega, kaj spletne storitve zagotavljajo. Spletne trgovine ne morejo sprejemati naročil, banke ne morejo ponujati e-storitev, javna uprava ne more sprejemati zahtevkov državljanov, podjetja lahko izgubijo povezavo s ključnimi sistemi preko API povezav itd.
- Nastane **finančna škoda** zaradi izpada prihodkov in **posredna škoda** zaradi izgube strank, okrnjenega ugleda podjetja, zamujeni roki pri upravnih zadevah itd.
- DDoS napadi ne vdrejo v notranjost omrežja in ne kradejo podatkov, povzročajo pa veliko težav, ker **smo izjemno odvisni od spletnih storitev**, lastnih in storitev drugih.

ZAŠČITA PRED DDOS NAPADI

Najbolj učinkovita je kombinacija DDoS zaščite pri ponudniku internetnih storitev in lastne zaščite.



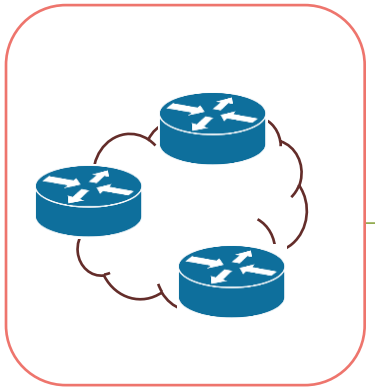
CELOVITA DDOS ZAŠČITA

Najbolj celovita DDoS zaščita vključuje kombinacijo zaščite v več točkah.

Oblak

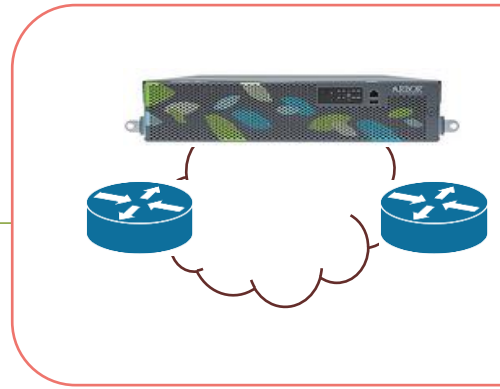
Zaščita v oblaku

Blokiranje volumetričnih, protokolnih in aplikativnih napadov.



Globalni Internetni ponudnik

Blokiranje volumetričnih napadov velikega obsega



Lokalni Internetni ponudnik

Blokiranje volumetričnih, protokolnih in delno aplikativnih napadov.

Organizacija

Blokiranje protokolnih in aplikativnih napadov. SSL dekripcija

PRIPOROČENI UKREPI OB NAPADU

Ob DDoS napadu je priporočeno izvajati sledeče ukrepe

- Spremljajte in beležite promet, ki je del napada.
- Glede na značilnosti napada, skupaj z Internetnim ponudnikom DDoS zaščite preverite, ali lahko naredite bolj učinkovite filtre prometa, ki bodo zmanjšali učinek napada.
- Zaščitite javno dostopne strežnike, premaknite jih na drugo, neprizadeto omrežje, ali za njih (začasno) najemite CDN storitev.
- Nemudoma obvestite SI-CERT ali SIGOV-CERT in pošljite kopije morebitnih izsiljevalskih sporočil ali druge povezane korespondence in podatke o značilnostih napada.
- V primeru izsiljevanja z izsiljevalci ne komunicirajte in predvsem ne plačajte odkupnine.

PREVERJANJE ODPORNOSTI PRED DDOS NAPADI

Priporočeno je izvajati preverjanje ali so storitve odporne na DDoS napade.

- Določiti sisteme in storitve ki so lahko tarča DDoS in so predmet preverjanja.
- Pregled obstoječe zaščite in nastavitev na NGFW, WAF, strežnikih, pri ponudniku interneta, v oblaku...
- Pripraviti plan testiranja in obvestiti vodstvo, skrbnike, hosting ponudnike.
- Izvedba aktivnega testiranja z generiranjem prometa proti sistemom in storitvam, vnaprej najavljeno in kontrolirano.
- Spremljanje učinkovitosti, spremembe nastavitev obstoječe zaščite in ponovno testiranje.
- Analiza rezultatov testa in izdelava poročila, ugotavljanje pomanjkljivosti in predlogi izboljšav, dodatnih ukrepov.

DDOS STATISTIKA ZA SLOVENIJO

SLOVENIA DDOS SUMMARY

2025

Month | Quarter | Year

Highlights:

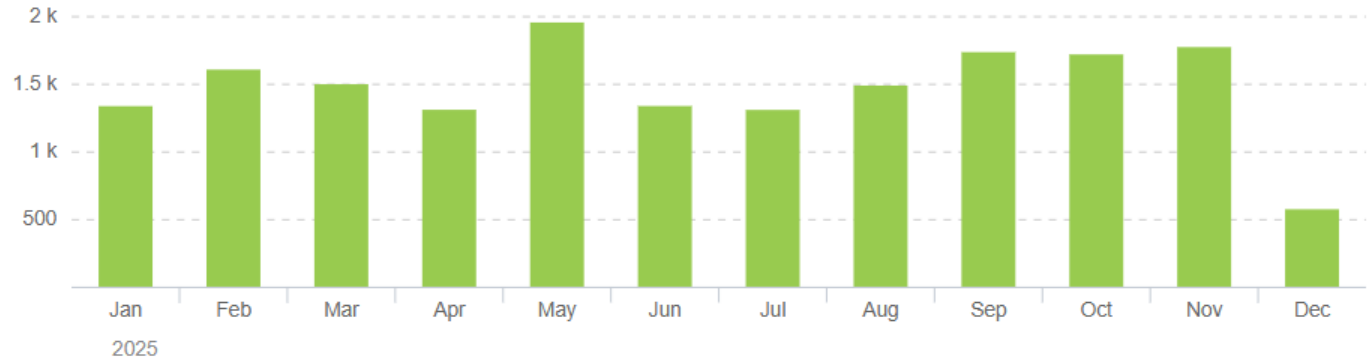
Attacks:	17.7 k
Peak Volume:	568 Gbps
Peak Speed:	233 Mpps
Peak Duration:	36 days (35 days, 23 hours)
Top Attack Types:	Total Traffic
	UDP
	DNS Amplification

https://horizon.netscout.com/

DDOS STATISTIKA ZA SLOVENIJO

FREQUENCY

Attack Frequency:

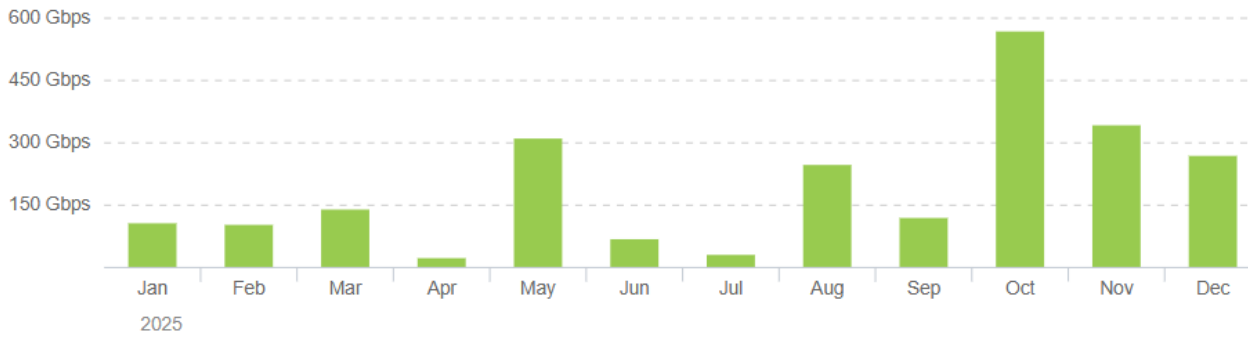


Frequency by Duration:

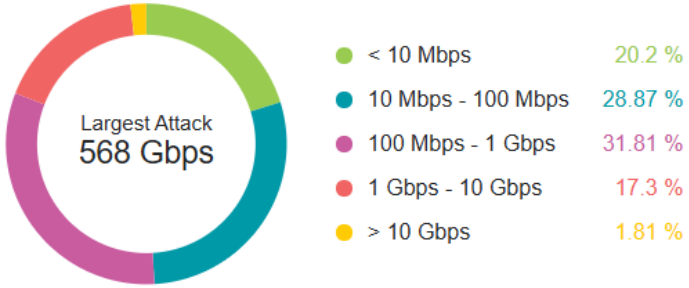
DDOS STATISTIKA ZA SLOVENIJO

VOLUME

Peak Attack Volume:

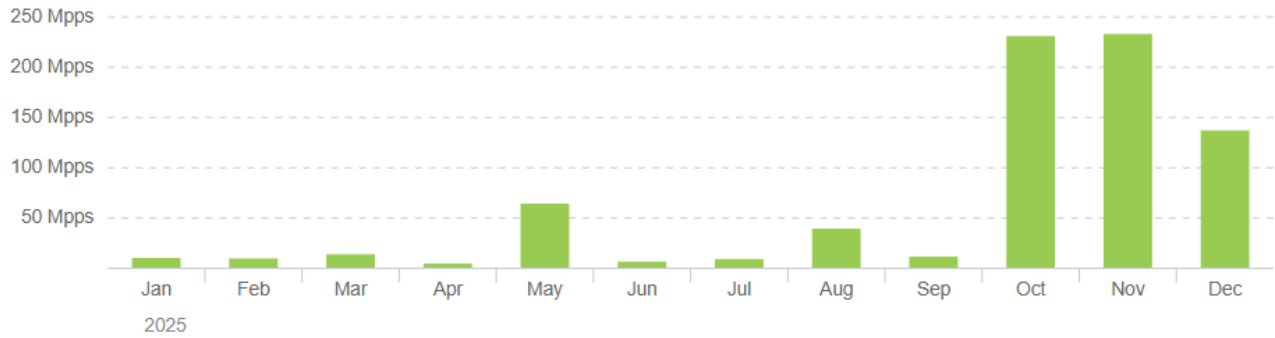


Breakout by Volume:

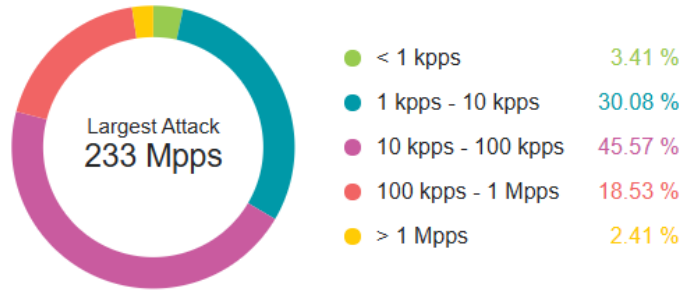


SPEED

Peak Attack Speed:



Breakout by Speed:



HVALA

+111 123 456 789

info@enisa.europa.eu