KIBERNETSKI CUNAMI:

Uničujoča moč DDoS napadov

Zoom platforma, 6. junij 2024, 14:00–15:00

zit SeKV
Združenje za informatiko in telekomunikacije
Kibernetska varnost

Gospodarska zbornica Slovenije

zit Združenje za informatiko in telekomunikacije

SRIP GoDigital

Sofinancira Evropska unija

I FEEL SLOVENIA

„Naložbo sofinancira Evropska unija iz Evropskega sklada za regionalni razvoj“

zit SeKV
Združenje za informatiko in telekomunikacije
Kibernetska varnost

Agenda:

14:00-14:05	**Uvodni pozdrav** Mihael Nagelj, predsednik Sekcije za kibernetsko varnost
14:05-14:20	**Opis fizionomije DDoS napadov** Jernej Bunič, Kontron d.o.o
14:20-14:45	**Izvajanje ukrepov – identifikacija, ukrepanje ob napadu (uporabnik storitve – žrtev napada)** Anton Brne, URSIV in Uroš Majcen, Kontron d.o.o.
14:45-14:55	**Večplastna strategija obrambe** Metod Platiše, Telekom Slovenije d.d.
14:55-15:00	Zaključek

KIBERNETSKI CUNAMI:

Uničujoča moč DDoS napadov

Zoom platforma, 6. junij 2024, 14:00–15:00

zit SeKV
Združenje za informatiko in telekomunikacije
Kibernetska varnost

Gospodarska zbornica Slovenije

zit Združenje za informatiko in telekomunikacije

SRIP GoDigital

Sofinancira Evropska unija

I FEEL SLOVENIA

„Naložbo sofinancira Evropska unija iz Evropskega sklada za regionalni razvoj“

kontron

&

zit SeKV

Združenje za informatiko in telekomunikacije
Kibernetska varnost

DOS & DDOS

Jernej Bunić
Svetovalec za kibernetsko varnost

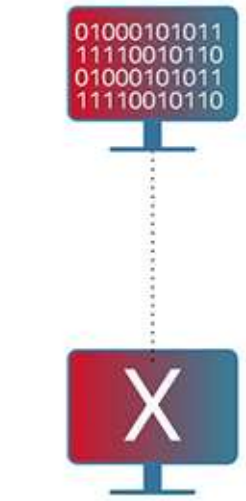
Kaj je Dos napad

› Denial of service

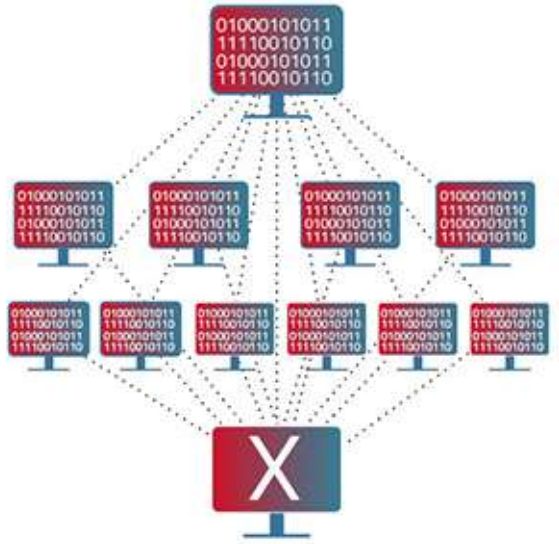
Gre za vrsto kibernetsekga napada, katerega cilj je onemogočiti eno ali več storitev

Ločimo dve vrsti Dos napada

- DOS – napad se izvaja iz enega vira (postaja tipično za zlorabo ranljivosti)
- DDOS – napad se izvaja iz mnogih virov (tipično za volumetrične napade, poplavne in amplifikacijske efekte)



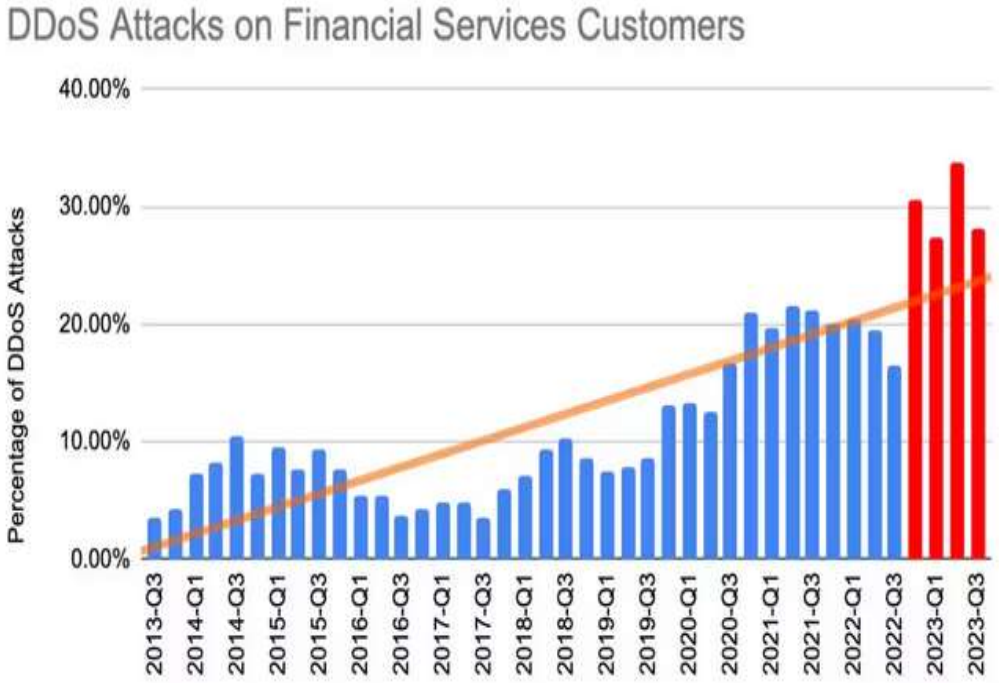
DoS attack



DDoS attack

Zakaj Dos napad

› Izsiljevanje – poslovni model



› Protest – ideologija

SLOVENIJA

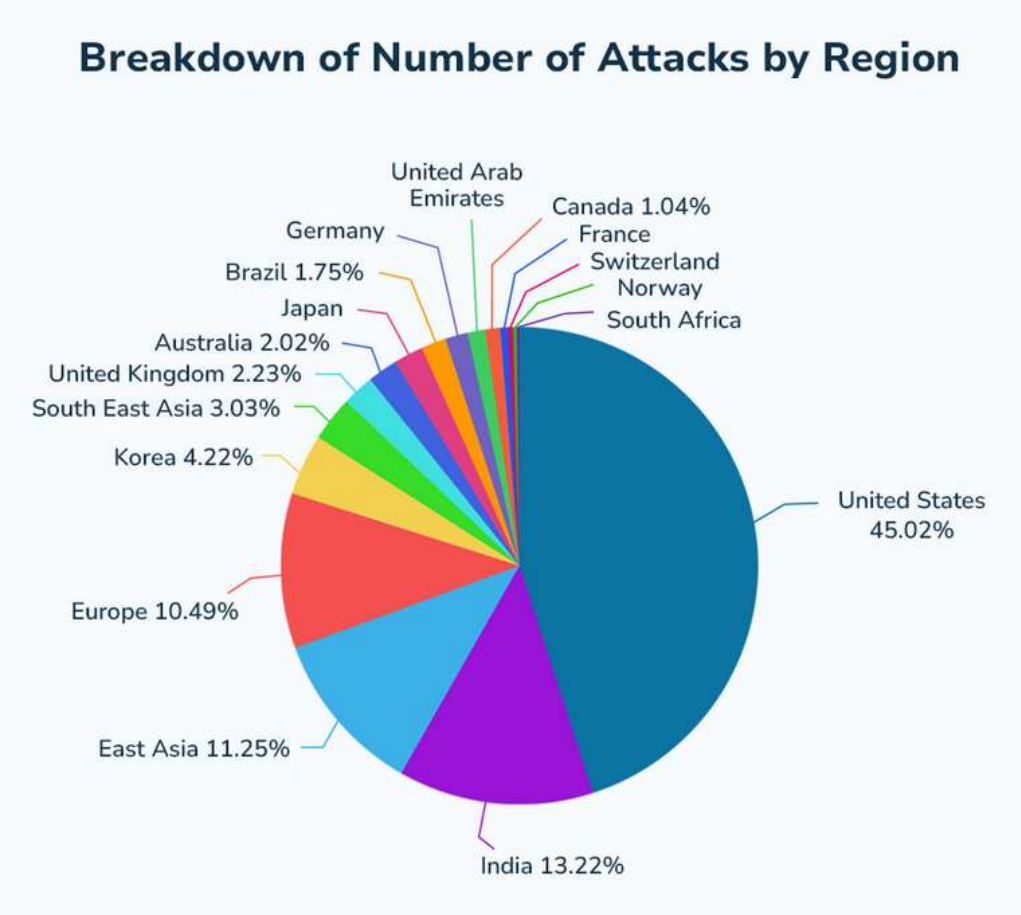
Ruski hekerji napovedali 'vojno' Sloveniji, napadli stran predsednice

Ljubljana, 27. 03. 2024 16.15 | Posodobljeno pred 18 dnevi

What Motivates Hacktivists?

Primarily hacktivism is sparked by an individual's or group's perception of what they consider to be 'wrong' or 'unjust' and hence incentivizes them to do something about it. Motivations include revenge, political or social incentives, ideology, protest, a desire to embarrass certain organizations or individuals within those organizations or sometimes sheer vandalism.

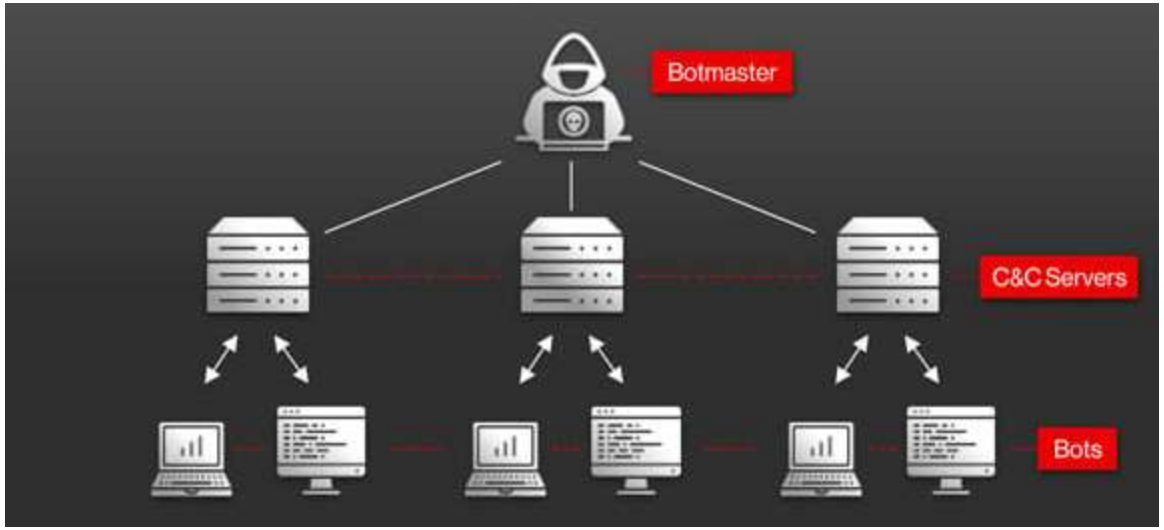
Povečanje Ddos napadov po 2020



- Organizacije spremenijo model poslovanja zaradi COVID19 pandemije, napadalci sledijo
- Porast IoT naprav poveča število potencialnih bot naprav
- Spremembe v svetovni geopolitiki
- Večnamenska raba botnetov

Botnet

› Botnet-I so večnamesnko orodje



- Spam napadi/kampanje
- Generiranje prometa
- Generiranje klikov
- Kripto rudarjneje
- Izvajanje Dos napadov
- Najemni model (stresser, dossers)

Telefoni!!!

Botnet

› Sestava in komunikacija

Iz arhitekturnega vidika sta dva glavna modela:

Odjemalec – strežnik
- Najbolj razširjena vrsta botneta

P2P
- Naprednješa oblika botneta – član ima lahko fukcijo strežnika ali klienta

Upravljanje:

- Centralizerano ali decentralizerano

Navadno je botnet sestavljen iz obeh modelov. Vse populrnejši je decentralizeran model
Botmaster ali botherder s člani komunicira prekorazličnih protokolov – telent, IRC, SMTP, domene, socialni mediji, GitHub

DDos

› Vrste napadov

Obstaja veliko tehnik kako izvesti Ddos napad. V grobem jih je možno razdeliti v tri vrste

- Aplikacijski nivo
  - Cilj je porabiti vse resorje strežnika, da ta ne more več odgovarjati na legitimne zahteve
  - Zahtevajo vzpostavljeno TCP povezavo (spoofanje ni mogoče)
  - Postajajo vse bolj popularni zaradi učinkovitejšega delovanja
- Omrežni nivo L4
  - Cilj je porabiti vse resorje strežnika ali povezovalne tabele
  - Ne potrebujejo vzpostavljene TCP seje (uporaba spoofanja)
  - Še vedno popularni in podirajo kolčinske rekorde
- Volumetrični
  - Poraba celotne pasovne širine žrtvinega internetnega dostopa
  - Proti tarči se pošlje Velika količina podtakov
  - Uporaba amplifkacijskih mehanizmov (DNS, NTP, Memcached…)

*Obstajajo vrste Dos napadov ki ne potrebujejo botneta – Memcached napad amplifikacija x50k

DDos

› Omrežni napadi

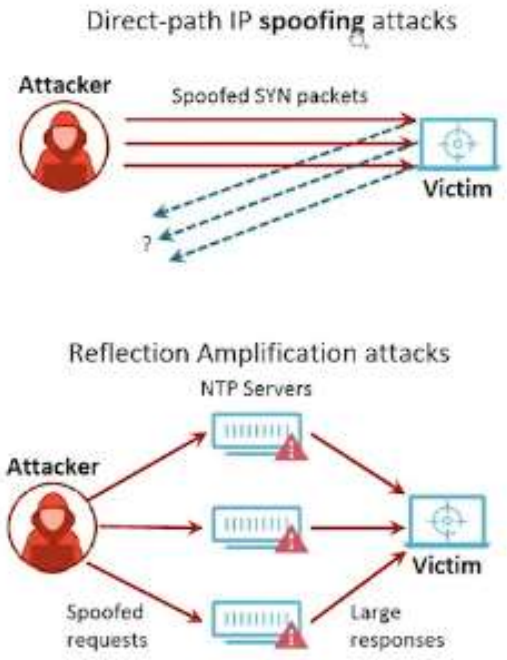
SYN flood

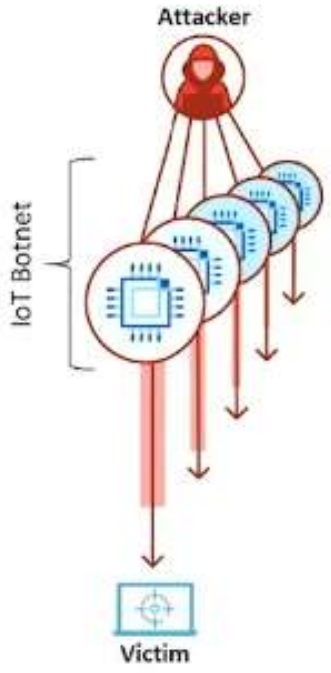
UDP flood

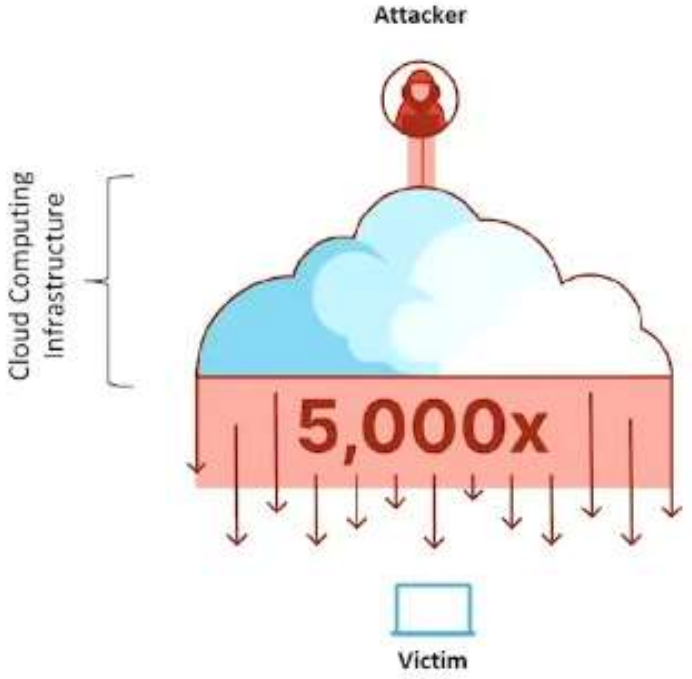
DNS flood

RST flood

Amplifikacijski napadi







Obstajajo vrste Dos napadov ki ne potrebujejo botneta – Memcached napad; amplifikacija x50k -1,3 Tbs

Rekord 3,47Tbs – Azure napad; UDP amplifikacijski napad uporaba SSDP, CLDAP, DNS in NTP. Trajal 15 min
Sestavljen iz cca 10.000 botov

DDos

› Aplikacijski napadi

- Naključni http flood
- http flood ki zaobide predpomnilnik storitve
- Low in slow attack
- Slow post
- HTTP2 napad

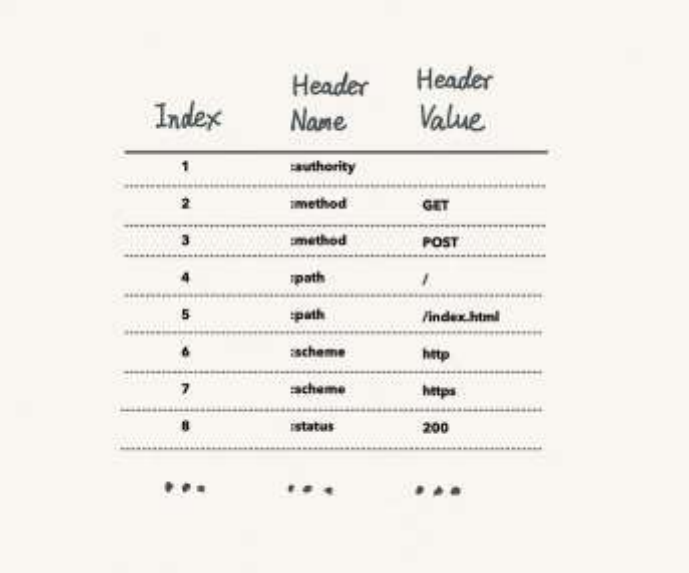
- Large Payload POST
- Mimicked user browsing

Potrebujemo vpogled v sejo - TLS

DDos

› HTTP2

- TLS je dvignil nivo varnosti
- HTTP/2 dvigne nivo učinkovitosti – lasnost ki se jo al izrablja tudi v slabe namene
- Uporaba statičnih in dinamičnih tabel, uporaba binarnrga formata namesto ASCII kode
- Uporaba kompresije glave - HPACK



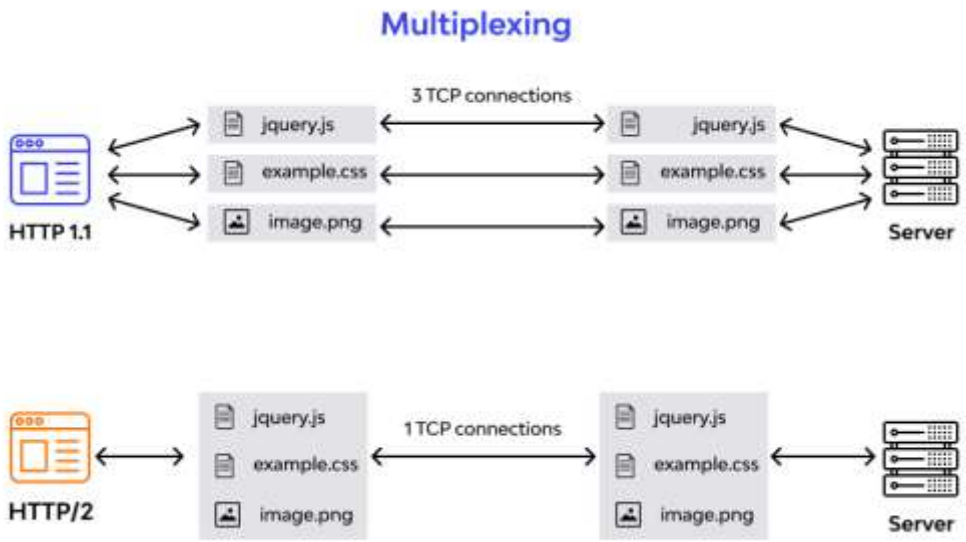
Index	Header Name	Header Value
1	:authority	
2	:method	GET
3	:method	POST
4	:path	/
5	:path	/index.html
6	:scheme	http
7	:scheme	https
8	:status	200

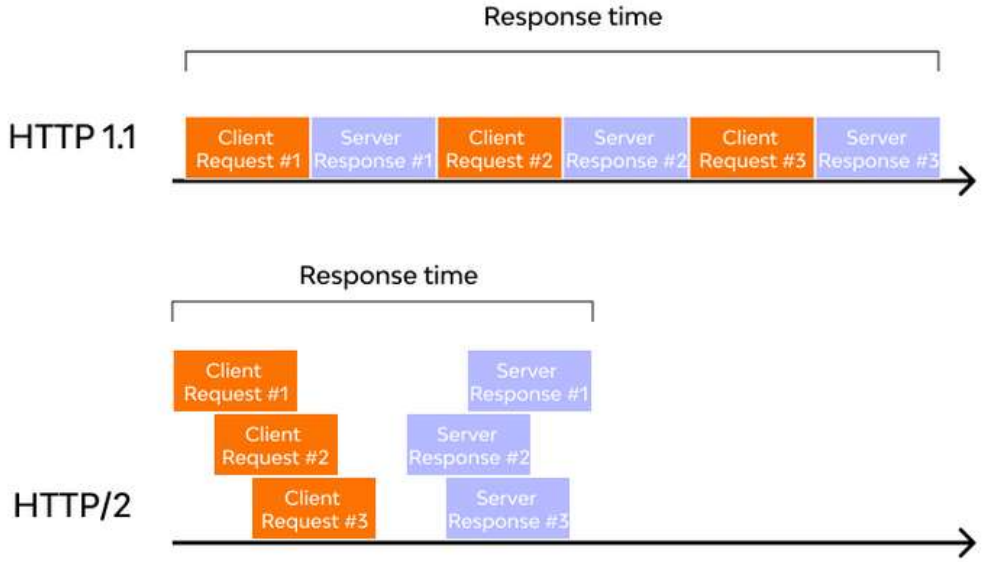
HTTP/2 Frame Type Specification

0x0 DATA	**RFC 7540**: Hypertext Transfer Protocol Version 2
0x1 HEADERS	**RFC 7540**: Hypertext Transfer Protocol Version 2
0x2 PRIORITY	**RFC 7540**: Hypertext Transfer Protocol Version 2
0x3 RST_STREAM	**RFC 7540**: Hypertext Transfer Protocol Version 2
0x4 SETTINGS	**RFC 7540**: Hypertext Transfer Protocol Version 2
0x5 PUSH_PROMISE	**RFC 7540**: Hypertext Transfer Protocol Version 2
0x6 PING	**RFC 7540**: Hypertext Transfer Protocol Version 2
0x7 GOAWAY	**RFC 7540**: Hypertext Transfer Protocol Version 2
0x8 WINDOW_UPDATE	**RFC 7540**: Hypertext Transfer Protocol Version 2
0x9 CONTINUATION	**RFC 7540**: Hypertext Transfer Protocol Version 2
0xa ALTSVC	**RFC 7838**: HTTP Alternate Services
0xc ORIGIN	**RFC 8336**: The ORIGIN HTTP/2 Frame

DDos

› HTTP2


Multiplexing
3 TCP connections
jquery.js
example.css
image.png
jquery.js
example.css
image.png
HTTP 1.1
Server
HTTP/2
jquery.js
example.css
image.png
1 TCP connections
jquery.js
example.css
image.png
Server

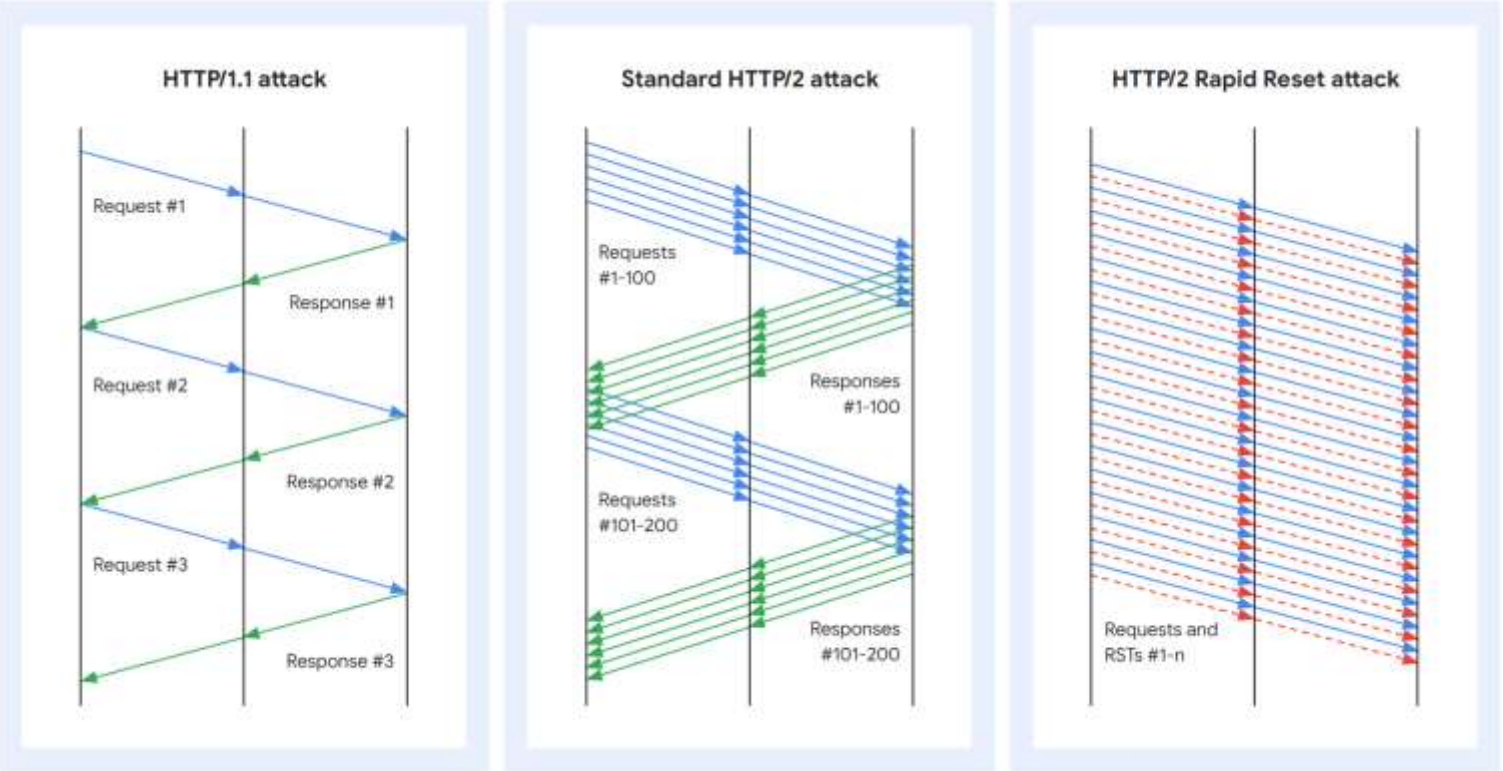

Response time
HTTP 1.1
Client Request #1
Server Response #1
Client Request #2
Server Response #2
Client Request #3
Server Response #3
Response time
HTTP/2
Client Request #1
Client Request #2
Client Request #3
Server Response #1
Server Response #2
Server Response #3

DDos

› HTTP2

The HTTP/2 Rapid Reset attack
CVE-2023-44487

- Veliko število “in-flight” zahtev
- Ker se takoj za zahtevo pošlje reset napad ni več odvisen od RTT ampak pasovne širine
- Strežnik porabi veliko resorjev -alokacija novih streamov, parsanje zahtev, dekomresija glave, mapiranje URLja
- RST_STREAM ne zahteva odgovora strežnika, manjša downlink poraba



Rekord 398 rps – Google

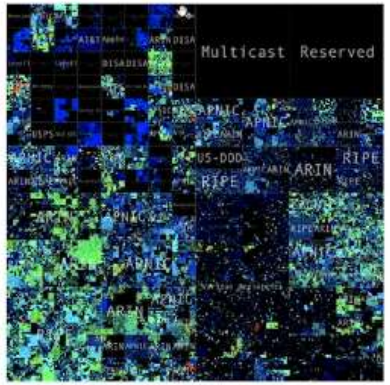
DDos

HTTP2

- **CVE-2024-27983**: Affects Node.js HTTP/2 server. Sending a few HTTP/2 frames can cause a memory leak due to a race condition, leading to a potential DoS.
- **CVE-2024-27919**: Affects Envoy's oghttp codec. Unlimited memory consumption due to not resetting a request when header map limits are exceeded.
- **CVE-2024-2758**: Relates to Tempesta FW. Its rate limits are not effectively preventing empty CONTINUATION frames attacks, potentially allowing DoS.
- **CVE-2024-2653**: Affects amphp/http. It collects CONTINUATION frames in an unbounded buffer, risking an OOM crash if the header size limit is exceeded.
- **CVE-2023-45288**: Affects Go's net/http and net/http2 packages. Allows an attacker to send an arbitrarily large set of headers, causing excessive CPU consumption.
- **CVE-2024-28182**: Involves an implementation using nghttp2 library, which continues to receive CONTINUATION frames, leading to a DoS without proper stream reset callback.
- **CVE-2024-27316**: Affects Apache Httpd. Continuous stream of CONTINUATION frames without the END_HEADERS flag set can be sent, improperly terminating requests.
- **CVE-2024-31309**: Affects Apache Traffic Server. HTTP/2 CONTINUATION DoS attack can cause excessive resource consumption on the server.
- **CVE-2024-30255**: Affects Envoy versions 1.29.2 or earlier. Vulnerable to CPU exhaustion due to a flood of CONTINUATION frames, consuming significant server resources.

Mitigacija

Kako se lahko borimo proti botnetom?



IPs that appear in
HTTP requests

IPs that appear in
Layer-4 DoS packets

Network Working Group
Request for Comments: 2827
Obsoletes: 2267
BCP: 38
Category: Best Current Practice

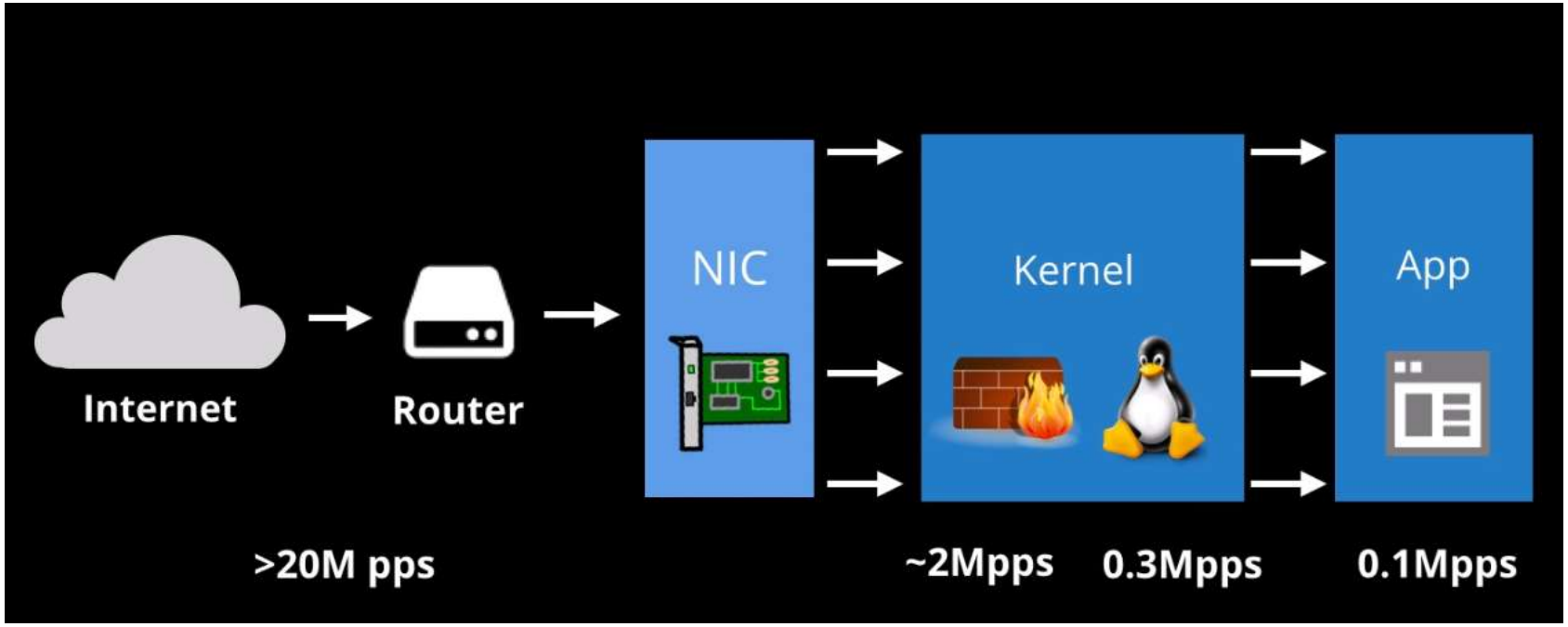
P. Ferguson
Cisco Systems, Inc.
D. Senie
Amaranth Networks Inc.
May 2000

Network Ingress Filtering:
Defeating Denial of Service Attacks which employ
IP Source Address Spoofing

ISP - Najboljša točka za obrambo pred L4 in edina toča zaščite pred volumetričnimi napadi

Mitigacija

Kaj lahko naredijo organizacije



- Routing – anycast/black hole (null route)
- Aplikacijo razdeliti med več IP-jev (TTL)
- Rate limiting
- Geo blokade

- Implementacija reverse-proxya
- “Hardening” naprav in servisov
-

Kako se lotimo Ddos zaščite

Odvisno od organizacije/podjetja in dejavnosti ki jo opravlja – pri odgovorih je potrebno upoštevati

- BIA
- RA
- Storitveni katalog z drevesi odvisnoti
- Določiti RPO in RTO-je za service
- Pregled obstoječe oprema in arhitekture

Vsaka organizacija ima svojo specifiko

kontron

WEBINAR JE OMOGOČILA

zit SeKV

Združenje za informatiko in telekomunikacije
Kibernetska varnost

kontron

FOR THE COMMUNITY, WITH THE COMMUNITY, BY THE COMMUNITY

KIBERNETSKI CUNAMI:

Uničujoča moč DDoS napadov

Zoom platforma, 6. junij 2024, 14:00–15:00

zit SeKV
Združenje za informatiko in telekomunikacije
Kibernetska varnost

Gospodarska zbornica Slovenije

zit Združenje za informatiko in telekomunikacije

SRIP GoDigital

Sofinancira Evropska unija

I FEEL SLOVENIA

„Naložbo sofinancira Evropska unija iz Evropskega sklada za regionalni razvoj“

zit SeKV
Združenje za informatiko in telekomunikacije
Kibernetska varnost

Agenda:

14:00-14:05	**Uvodni pozdrav** Mihael Nagelj, predsednik Sekcije za kibernetsko varnost
14:05-14:20	**Opis fizionomije DDoS napadov** Jernej Bunič, Kontron d.o.o
14:20-14:45	**Izvajanje ukrepov – identifikacija, ukrepanje ob napadu (uporabnik storitve – žrtev napada)** Anton Brne, URSIV in Uroš Majcen, Kontron d.o.o.
14:45-14:55	**Večplastna strategija obrambe** Metod Platiše, Telekom Slovenije d.d.
14:55-15:00	Zaključek

kontron

&

zit SeKV

Združenje za informatiko in telekomunikacije
Kibernetska varnost

Izvajanje ukrepov – identifikacija, ukrepanje ob napadu (uporabnik storitve žrtev napada

Uroš Majcen, Kontron d.o.o.
Anton Brne, URSIV SIGOV-CERT

Vloge

- SIGOV-CERT URSIV
  - Odzivni organ za varnostne incidente v državni upravi
- Kontron d.o.o.
  - Zunanji izvajalec SOC storitev

Najava DDOS dogodkov

Najava 27.03.2024

O CyberArmy Russia Reborn

Gre za preimenovani KillNet

- Organizirana skupina, poznana po izvedbi DDOS napadov
- https://en.wikipedia.org/wiki/Killnet
- Nekaj tipov DDOS napadov, ki jih izvajajo:
  - ICMP Flood
  - IP Fragmentation
  - TCP SYN Flood
  - TCP RST Flood
  - TCP SYN / ACK
  - NTP Flood
  - DNS Amplification
  - LDAP Connection less (CLAP).[4]

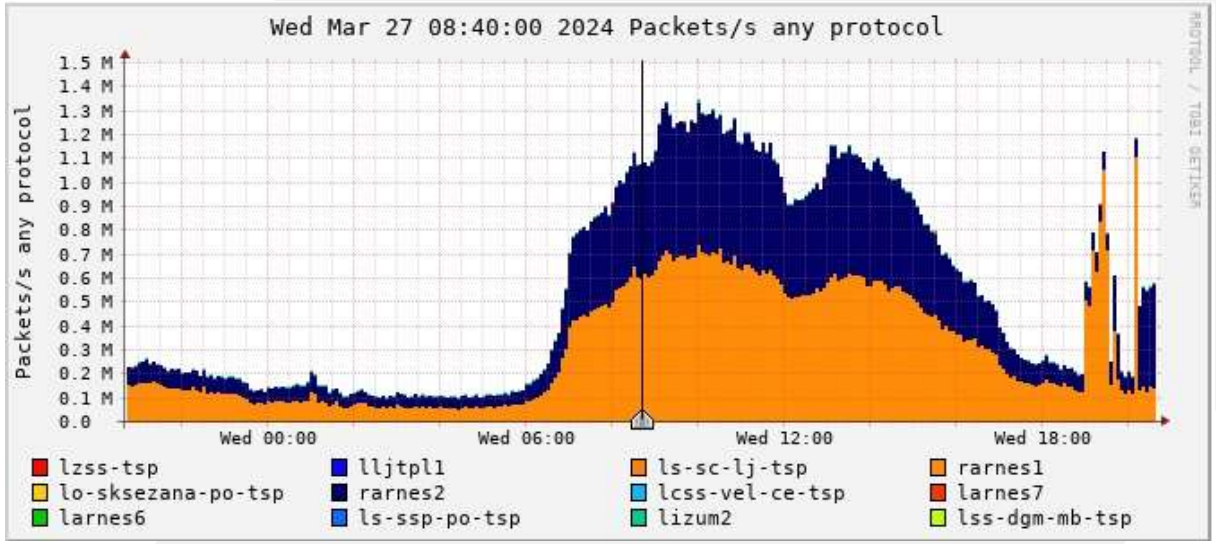
Killnet

Kaj pravijo TI viri o njih?

- What is Killnet?
  - "Killnet" is a financially- and ideologically-motivated threat group, likely based in Russia, that has committed distributed denial-of-service (DDoS) and data exfiltration attacks against Western entities and Dark Web markets.
    - First emerging in October 2021, Killnet initially offered for-hire DDoS attacks. Flashpoint observed the first ads posted by the group about its for-hire DDoS service in January 2022 on various Russian-language illicit forums.
    - Following Russia's February 2022 invasion of Ukraine, however, the collective started conducting, threatening, and taking responsibility for attacks on networks in Ukraine and in countries seen as supporting Ukraine. The group openly pledged allegiance to Russia, particularly in the context of the war. Killnet has stated its disdain toward NATO and Western weapons shipments to Ukraine.
  - Since February 2022, Killnet has targeted both state-owned and private websites. The group has also attacked networks in countries that provide assistance to Ukraine, or who have supported sanctions against Russia. The group's associates have also perpetrated hack-and-leak attacks against Ukrainian systems.

Kako žrtev vidi napad?

- Nadzorni sistemi:
  - Izpad delovanja spletne strani – nadzor razpoložljivosti
  - Povečana poraba sistemskih virov (CPU, RAM)
  - Nenadno povečanje količine podatkov v dnevniških datotekah



Kako žrtev vidi napad?

- Varnostni sistemi:
  - SIEM – podatki iz požarnih pregrad
- Uporabniki:
  - Izpad delovanja spletnih storitev

Bili smo obveščeni o napadu

Kaj pa sedaj?

- Ali imamo načrt za odziv na varnostni incident?
  - Runbook za DDOS napade?
- Ali smo dolžni prijaviti incident?
  - SIGOV-CERT/SI-CERT
- Identifikacija tipa DDOS napadov
  - Od tipa odvisna “mitigacija” in ukrepi
- Prvi korak, ki ga večina izvede:
  - Ponovni zagon spletnega strežnika (ne odpravi problema)

Napad na omrežje HKOM

- 3 valovi napadov, vsak je bil drugačen
- Volumentrični napad – oviranje delovanja spletnih storitev in izpad spletnih strežnikov
  - FURS
  - SURS
  - Storitve zaupanja (SIGEN-CA)
  - E-uprava
- Široka razvejanost in soodvisnosti
- Ciljni napadi spletišč
- Po identifikaciji tipa napada izvedbe različnih ukrepov
  - Geoblokade
  - Rate limiting
  - Iskanje IP napadalcev - > blokade
    - Prilagajanje, kot so se napadalci prilagajali

Izvedba ukrepov

Priporočila

- Izvedba ukrepov odvisna od tehničnih zmožnosti
  - Ali požarna pregrada omogoča “rate limiting”?
- Geoblokada: oster ukrep, ki mora biti resnično začasen
- Različne tehnične rešitve
  - WAF z dodatnimi funkcionalnostmi
- Varovanje spletišč z rešitvami, kot so “fail2ban”

kontron

WEBINAR JE OMOGOČILA

zit SeKV

Združenje za informatiko in telekomunikacije
Kibernetska varnost

kontron

FOR THE COMMUNITY, WITH THE COMMUNITY, BY THE COMMUNITY

KIBERNETSKI CUNAMI:

Uničujoča moč DDoS napadov

Zoom platforma, 6. junij 2024

zit SeKV
Združenje za informatiko in telekomunikacije
Kibernetska varnost

Gospodarska zbornica Slovenije

zit Združenje za informatiko in telekomunikacije

SRIP GoDigital

Sofinancira Evropska unija

I FEEL SLOVENIA

„Naložbo sofinancira Evropska unija iz Evropskega sklada za regionalni razvoj“

zit SeKV
Združenje za informatiko in telekomunikacije
Kibernetska varnost

Agenda:

14:00-14:05	**Uvodni pozdrav** Mihael Nagelj, predsednik Sekcije za kibernetsko varnost
14:05-14:20	**Opis fizionomije DDoS napadov** Jernej Bunič, Kontron d.o.o
14:20-14:45	**Izvajanje ukrepov – identifikacija, ukrepanje ob napadu (uporabnik storitve – žrtev napada)** Anton Brne, URSIV in Uroš Majcen, Kontron d.o.o.
14:45-14:55	**Večplastna strategija obrambe** Metod Platiše, Telekom Slovenije d.d.
14:55-15:00	Zaključek

Zaščita pred napadi DDoS

WEBINAR JE OMOGOČILA:

zit SeKV

Združenje za informatiko in telekomunikacije
Kibernetska varnost

Metod Platiše, metod.platise@telekom.si

TelekomSlovenije

DDoS skozi čas

1996 – Prvi DDoS-napad

SYN flood
Panix, NY ISP

2000 – Profi DDoS-napadi

botnet
Amazon, eBay, Yahoo, Dell, CNN, CIA

2007 – Država-država DDoS napadi

Rusija napadla Estonijo
S. Koreja napadla ZDA državne spletne strani

2016 – IoT postane orodje za DDoS, DDoSaaS

Zelo povečana zmogljivost do 1 Tb/s

2018 – RansomDDoS

Zahteva za odkupnino
Velika vztrajnost

2020 – AP advanced persistent Hibridni napadi

Različni motivi, zakritje drugega napada

2024 – Geopolitično motivirani napadi

Motiv propaganda, vznemirjenje, strah

https://horizon.netscout.com/ https://www.netscout.com/threatreport

DDoS-kampanja 2024

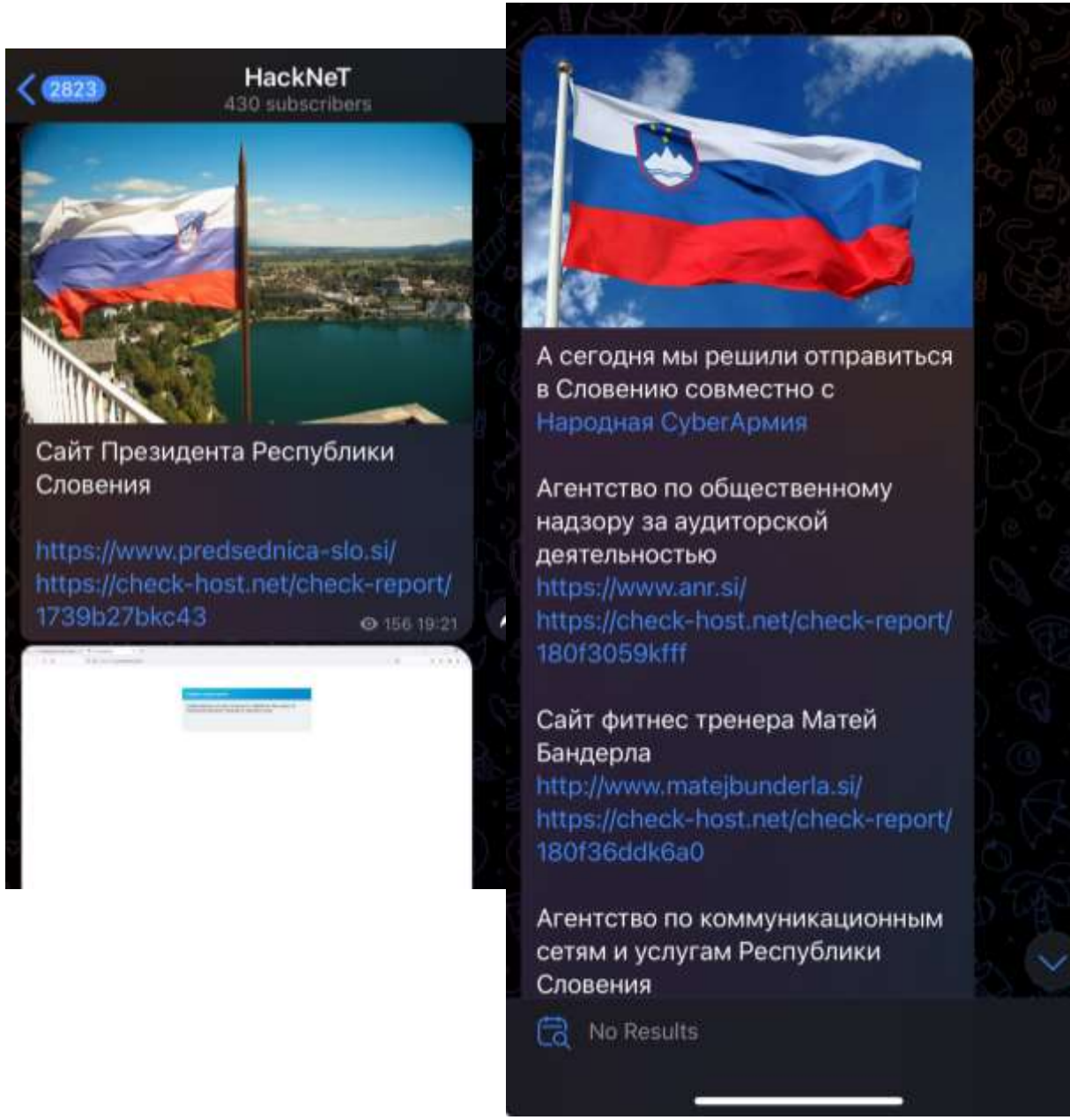
27. marec, skupina **Russian Cyber Army**

According to reports from close to reliable sources, **Slovenia has joined the Czech initiative to purchase ammunition for Ukraine**. This was announced by Czech Foreign Minister Jan Lipavsky. He did not name a specific amount of assistance, but earlier Slovenian media reported that the government could allocate €1 million. Let us recall that the Czech Republic, together with its partners, was able to raise part of the funds for the purchase of the first batch of artillery shells for Ukraine. We are talking about 300 thousand ammunition out of 800 thousand planned for delivery. **The People's CyberArmy □□ announces the start of massive attacks on the websites of government agencies of the Republic of Slovenia!** 🚫
SI🤝🐷UA Let's start with the website of the President of the Republic of Slovenia🐖 URL: https://www.predsednica-slo.si/
IP: 84.39.219.247 ‼️‼️Follow our publications, the list of DDoS targets will be updated! The main website of Slovenia fell at the hands of Russian hackers from the People's Cyber Army 😁
https://check-host.net/check-report/172326fak726

DDoS-kampanja 2024

29. marca se pridruži skupina **HackNet**
od 16. aprila dalje intenzivno izvaja napade

And today we decided to go to Slovenia together with the People's CyberArmy Agency for Public Supervision of Auditing Activities https://www.anr.si/ https://check-host.net/check-report/180f3059kfff
Website of fitness trainer Matej Banderla http://www.matejbunderla.si/ https://check-host.net/check-report/180f36ddk6a0 Agency for Communication Networks and Services of the Republic of Slovenia https://www.akos-rs.si/ https://check-host.net/check-report/180f54cdk7c9 Subscribe HackNet



TelekomSlovenije

DDoS-kampanja 2024

29. marca objavo posreduje skupina **NoName057(16)**
11. aprila se aktivno pridruži napadom

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

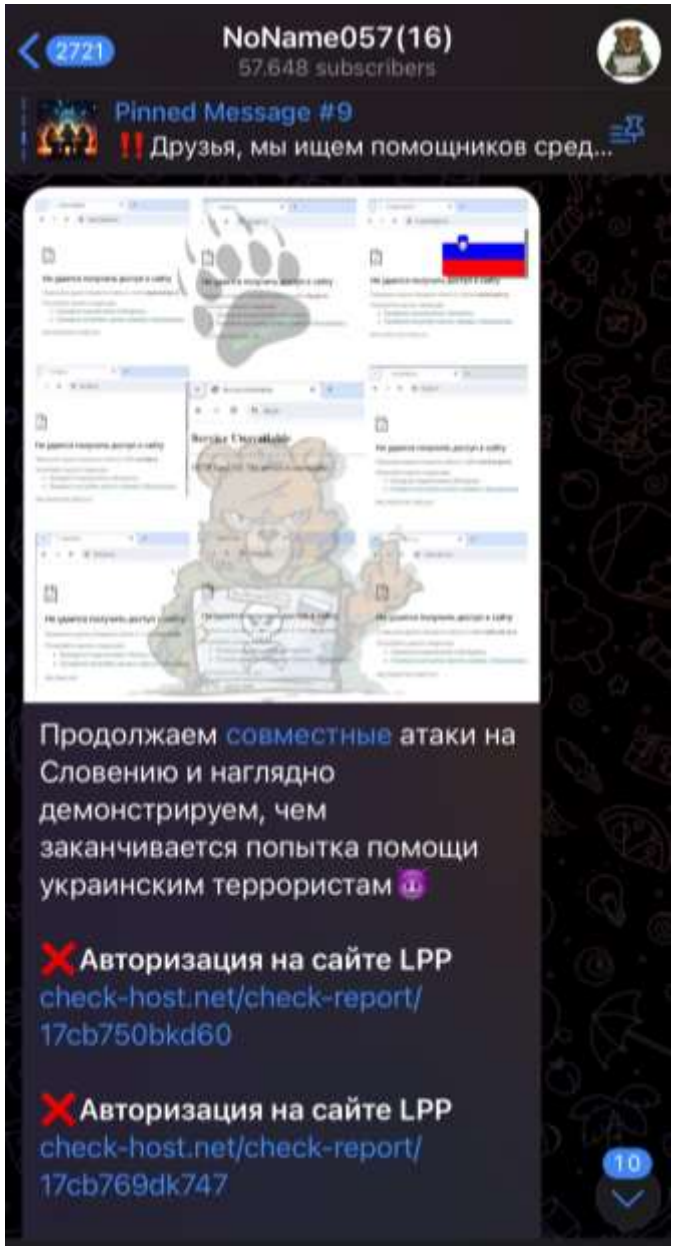
❌ Statistical Office of the Republic of Slovenia
check-host.net/check-report/17cc98c2kd19
❌ Ombudsman of the Republic of Slovenia (closed by geo)
check-host.net/check-report/17cc9bb8k69c
Subscribe ➡ NoName057(16) | DDoSia Project | Reserve | Eng version

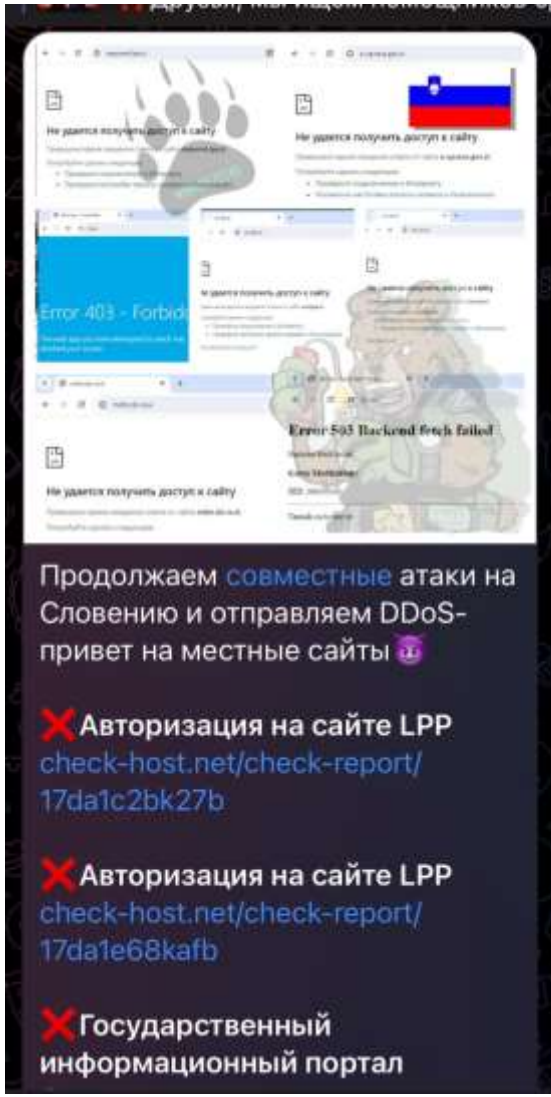
We continue our fascinating DDoS journey through the government websites of Slovenia 😈

❌ 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

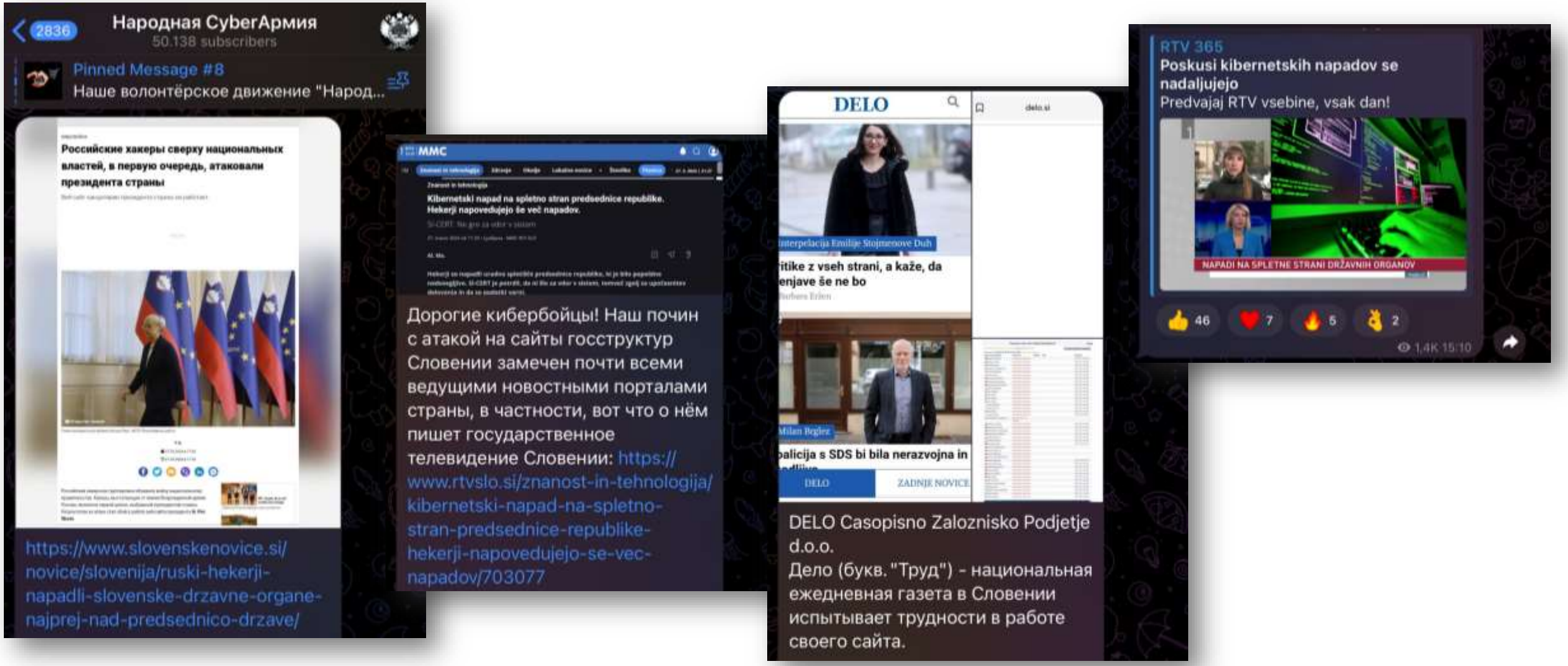




TelekomSlovenije

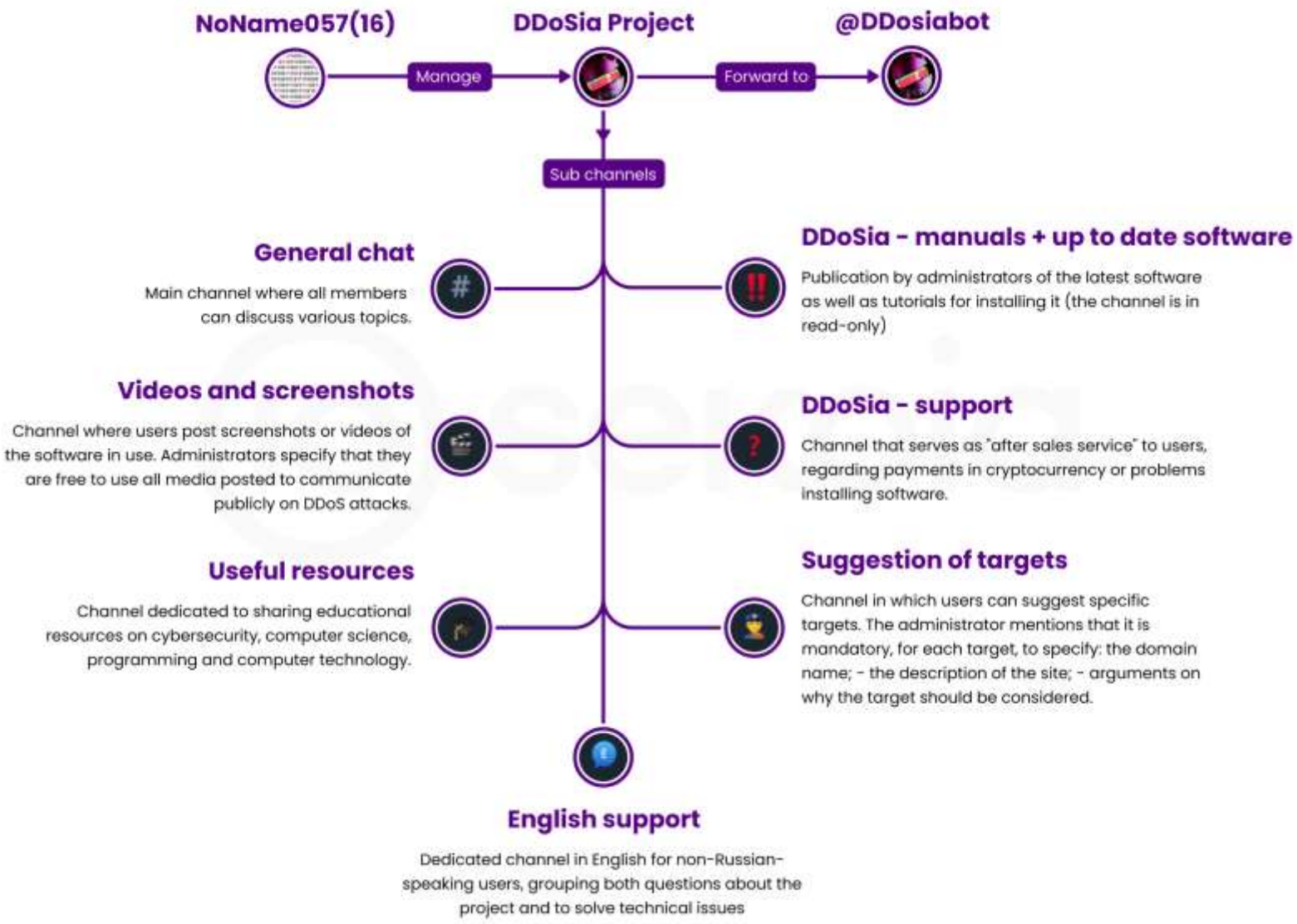
DDoS-kampanja 2024

Napadalci povzemajo slovenske medijske objave



TelekomSlovenije

sekoia | NoName057 Telegram channels



DDoS-kampanja 2024

People's Cyber Army of Russia
Our volunteer movement "People's Cyber Army of Russia" is announcing a fundraiser that will be used to purchase additional tools for the uninterrupted work of our specialists.
Many of you know that the fight against dill propaganda is extremely expensive and we cannot always cope on our own.
Anyone can help, and it's very easy to do.

In the purpose of the transfer, be sure to indicate “Charitable contribution for the NCA” or “Donation for the NCA”.

You can keep track of what is being purchased with the funds raised and ask questions through personal messages to the administration of our movement.

Volunteers are also needed with their own tools for the job.

Monero crypto wallet and bank card number for your support of the People's Cyber Army of the Russian FederationRU

Koshelek Monero:
4B3ZNG1VfeTCCVFSkE29gNK3ZJferHi6DfVZWqXkwr98D7gqP4gdyXQQKAtmxaH8uV6EYzMuPoen6Zspf37Ad2MQ5au1Kkx

Otkritie Bank card:
2200290573103604

DDoS-kampanja 2024

NoName057(16)

📌 Friends! The volunteers of our DDoSia Project and I daily and hourly rebuff the Russophobic West and its attempts to dictate conditions to us - FREE PEOPLE AROUND THE WORLD!!!😡

With our hard work, we remind governments of countries that have forgotten about the problems of their citizens that it is time to take care of the lives of ordinary people and stop "adding fuel to the fire" and throwing money into the furnace of the criminal regime of Ukraine!🔥

We decided not to stop in our good deeds)))

Our guys at the front are facing a decisive moment and we want to support them as much as possible, and this is not at all difficult.

We started a collab with DaZbastaDraw HIMSELF - the most popular artist-designer, the author of many well-known graphic works on the Internet and on the front, and a serious figure in collecting assistance for air defense soldiers

❗What you need to do: buy cool stickers with our bears from DaZBasta and thereby contribute to this story😎

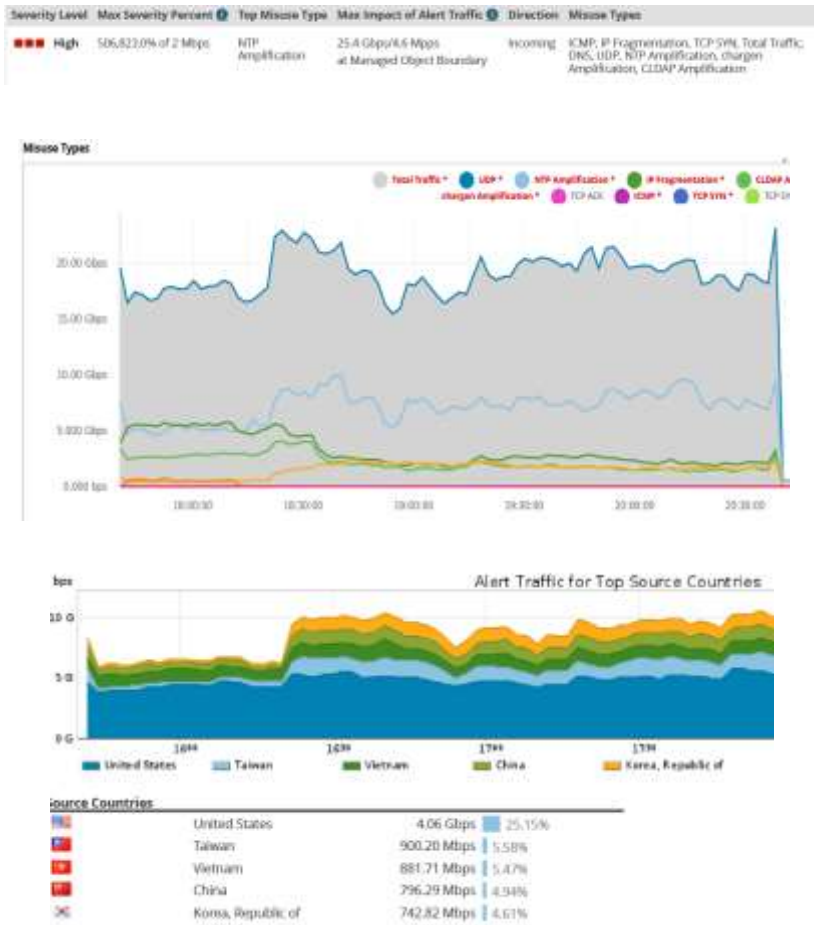
The proceeds will go to help SVO soldiers.

Further more! Stay tuned!😉

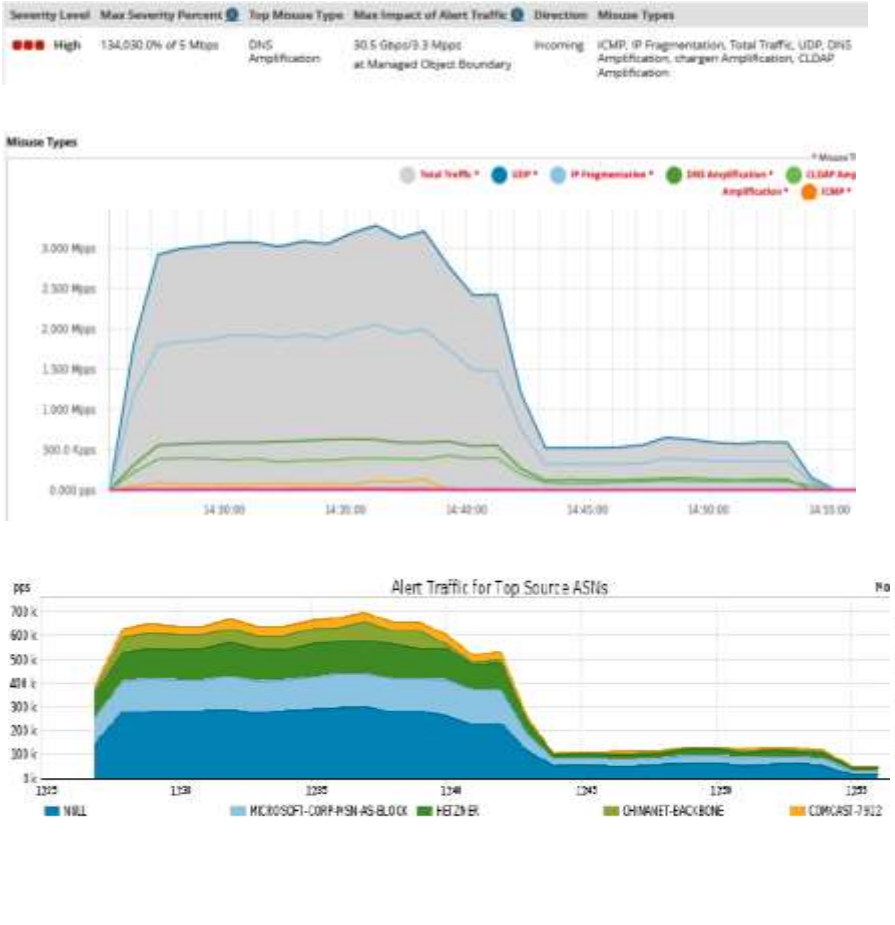
Subscribe ➡ NoName057(16)|DDoS project|Reserve|English

Večji napadi, ki smo jih zaznali pred leti

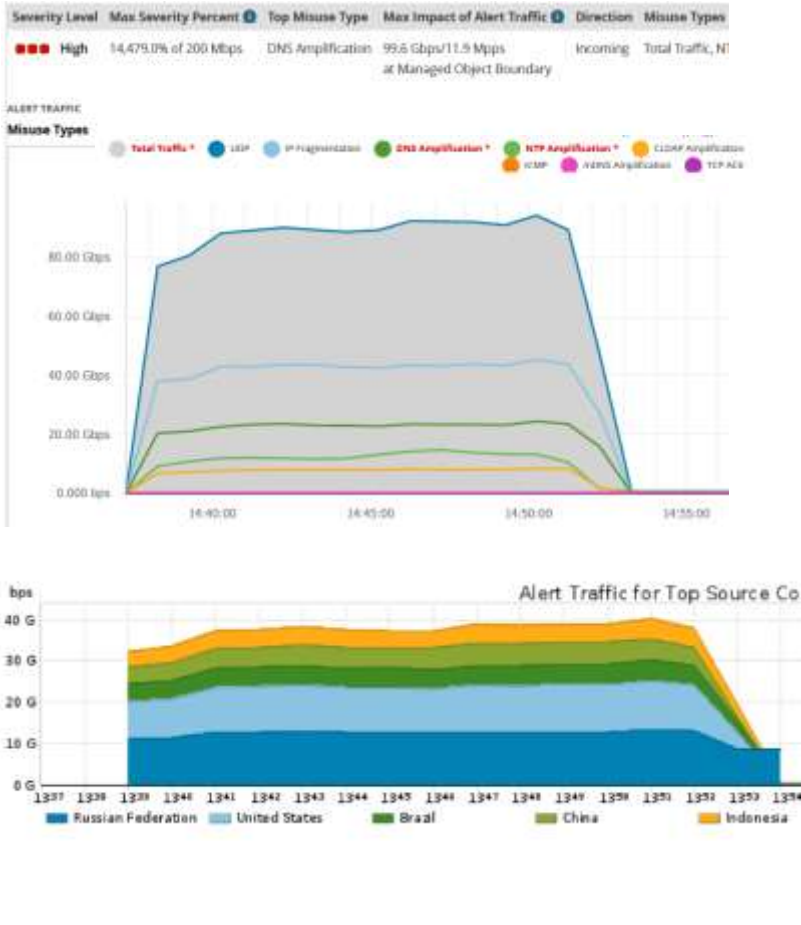
Napad na medijsko hišo



Napad na finančno inštitucijo



Napad na ponudnika storitev



TelekomSlovenije

Napadi v letošnji kampanji

Volumetrični napadi

Detekcija

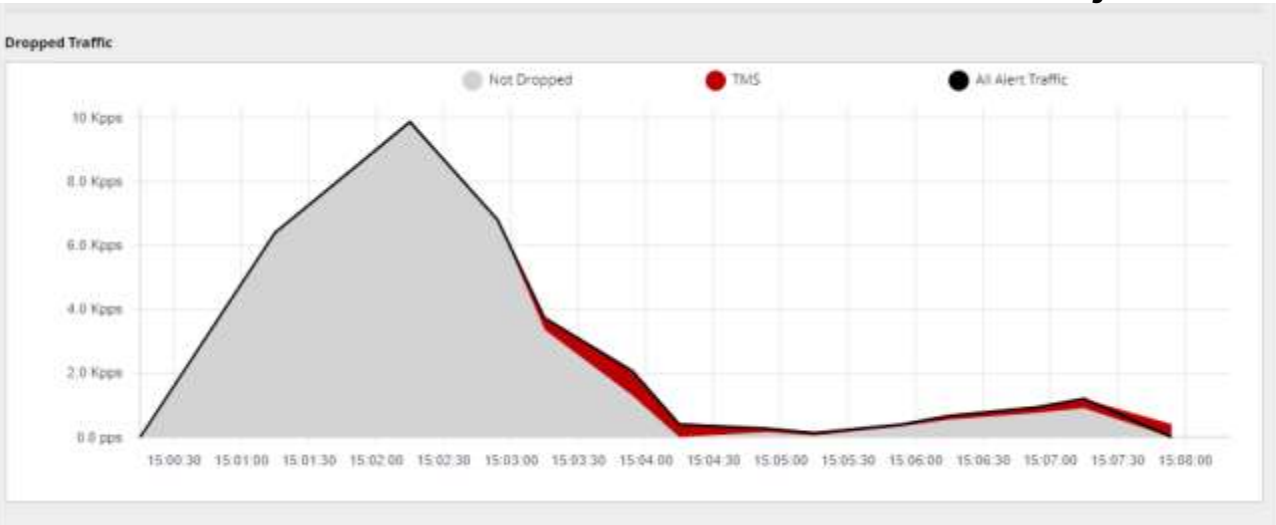
Mitigacija

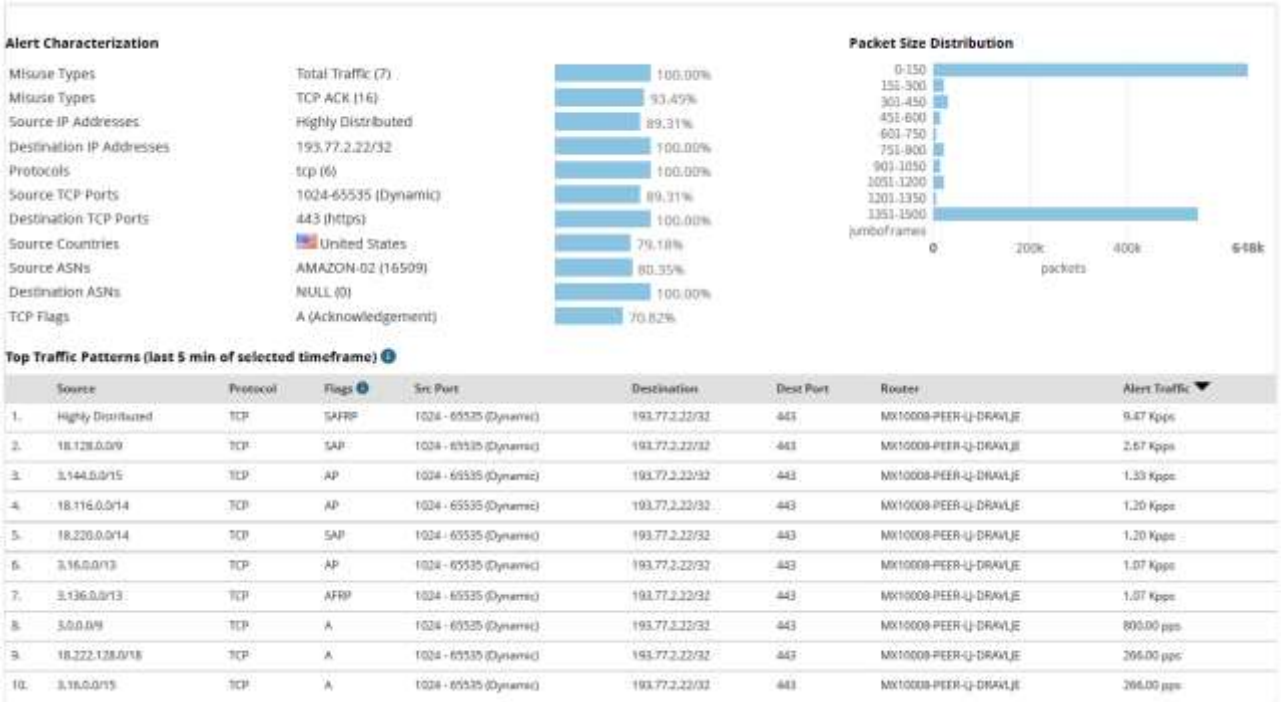
TelekomSlovenije

Napadi v letošnji kampanji

Aplikativni napadi

Detekcija





Mitigacija

TelekomSlovenije

Statistika DDoS dogodkov

NETSCOUT

SLOVENIJA DDOS SUMMARY

2024

Month | Quarter | Year

Highlights:

Attacks:	790
Peak Volume:	36.1 Gbps
Peak Speed:	5.85 Mpps
Peak Duration:	1 day (1 day, 10 hours)
Top Attack Types:	DNS Amplification
	IP Fragmentation
	UDP

https://horizon.netscout.com/?atlas=summary&hoods=destination.region.SI&y=2024

Statistika DDoS dogodkov

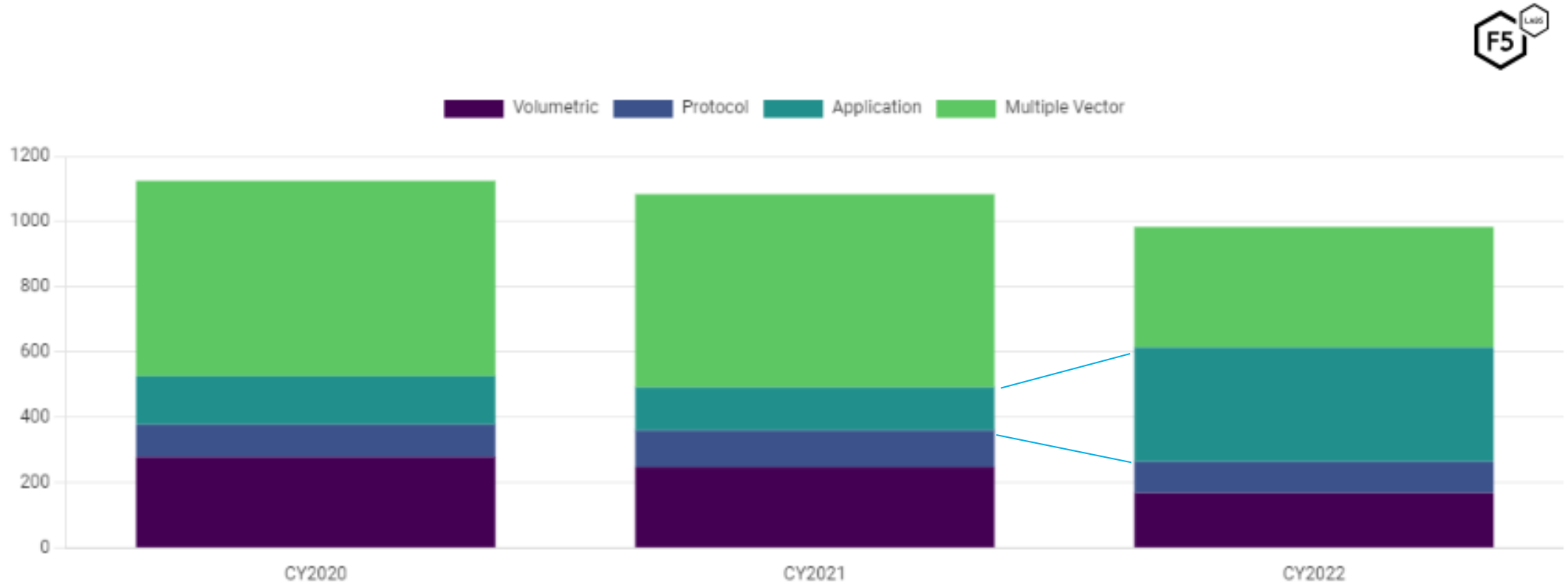


Figure 2 2020-2022 DDoS Attack Category counts. This shows a large increase in the number of Application attacks, with a corresponding reduction in Volumetric and Multiple Vector categories

[2023 DDoS Attack Trends | F5 Labs]

Anatomija napadov DDoS

Priprava

Napadalci analizirajo tarčo:

- identificirajo javne servise, spletne strani, DNS, VPN-dostope, izvedejo t. i. OSINT,
- identificirajo odvisne servise v oblaku, ISP-servise, tranzitne točke,
- identifi… pošljejo … zahteva… …iptovalutah.

Opozorilni napad

- Napadalci sprožijo krajši napad n… enega od servisov.
- Pošljejo izsilje… zagro…

…napad

- Napadalci sprožijo napad na več servisov hkrati.
- Spreminjajo tehnike (vektorje) tekom napada.
- Napad je dolgotrajen in konstanten.

Obsolete !

Značilnosti napadov

- Zmogljivost 50 - 300 Gbps, 150 Kpps – 10 Mpps.

Napadalci se poimenujejo ‘Fancy Bear’, ‘Lazarus Group’, ‘Armada Collective, aka LBA.

- Vektorji:
  - DNS
  - ntp
  - ARMS
  - WS-DD
  - SSDP
  - memcached
  - CLDAP reflection/amplification
  - UDP/4500 and UDP/500 flooding
  - HTTP/S request-flooding
  - spoofed SYN-flooding
  - **GRE & ESP packet-flooding**
  - TCP ACK-floods
  - TCP reflection/amplification attacks

!! Po nekaj mesecih napadalci ponovno izvedejo napade na nekatere tarče, ki se niso odzvale na izsiljevalsko sporočil !!

Kako se zaščititi pred napadi DDoS?

DDoS poskuša:

- zapolniti internetno povezavo:
  - ICMP, UDP, IPSec flood, odboj, ojačanje…

- onesposobiti požarno pregrado ali drugo ‘statefull‘ napravo:
  - SYN flood,
  - SSL Exhaustion,
  - DNS NXDOMAIN flood.

- onesposobiti spletni strežnik ali aplikacijo:
  - Slowloris, Slow POST, Slow READ,
  - Low and Slow,
  - ali pa se pretvarja in nastopa kot uporabnik.

DDoS Quick Guide (cisa.gov)

Kako se zaščititi pred napadi DDoS?

Poznavanje infrastrukture in spletnih storitev

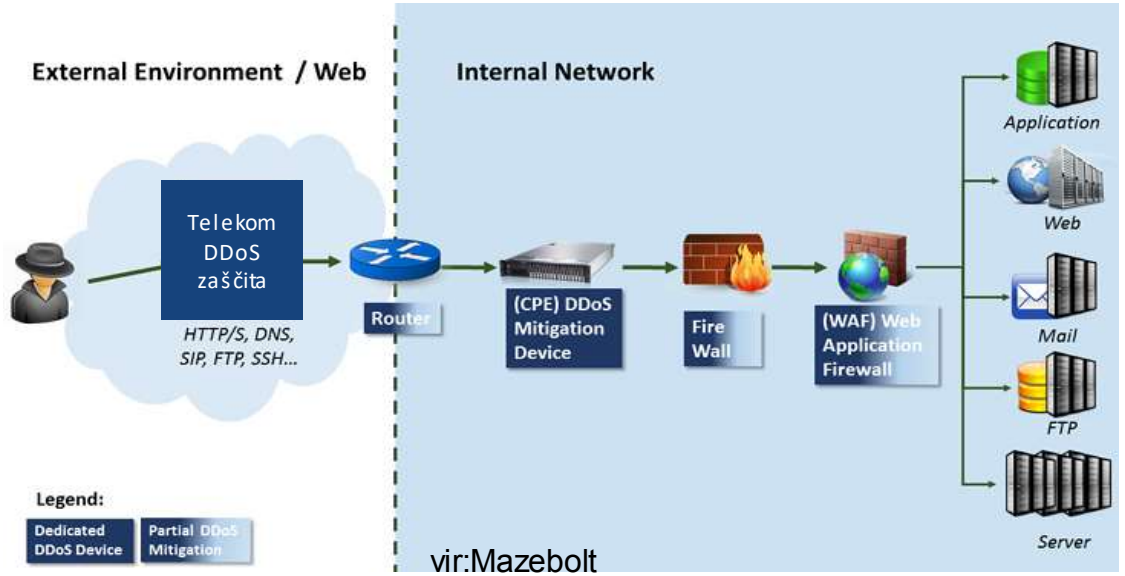
- Kakšne so vaše spletne storitve ?
- Od česa so storitve odvisne, koliko so zmogljive ?
- Kako smo vidni navzven?
- Kaj vam lahko napadejo?
- Utrditev varnosti na zunanjih napravah, spletnih strežnikih.

DDoS-zaščita Telekoma Slovenije

- Točka zaščite v omrežju Telekoma Slovenije.
- Visoka zmogljivost.
- Različni mehanizmi zaščite.
- Avtomatska mitigacija.
- Nadzor v Operativnem centru kibernetske varnosti.

DDoS-zaščita v podjetju

- DDoS-zaščitna naprava na internet dostopu v podjetju.
- DDoS mehanizni na WAF in SLB
- DDoS zaščita v oblaku

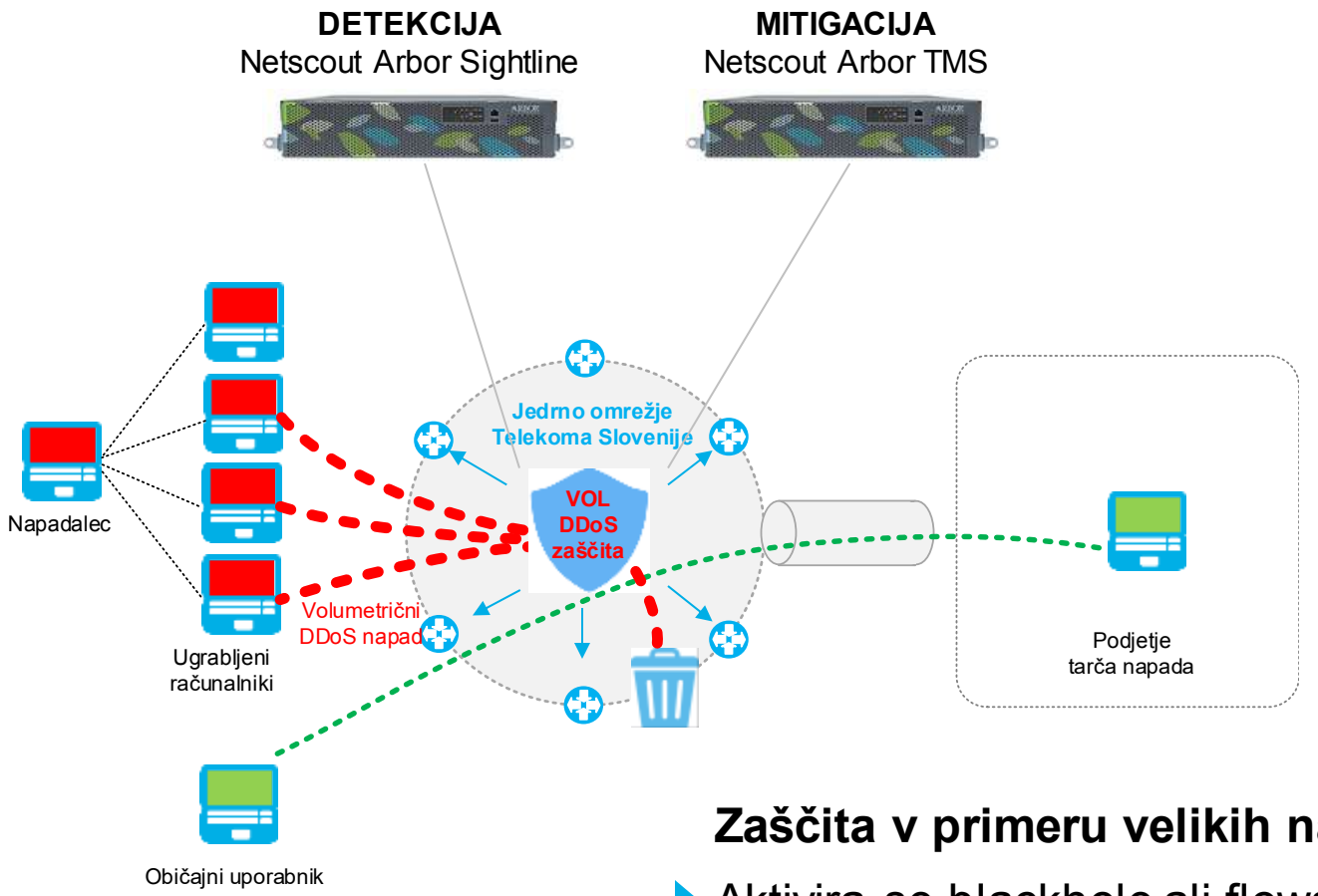


vir:Mazebolt

TelekomSlovenije

DDoS-zaščita Telekoma Slovenije

- Sistem za detekcijo zajema Netflow statistiko iz peering usmerjevalnikov.
- Ko sistem zazna anomalijo v prometu, generira alarm in preusmeri promet na sistem mitigacije.
- Sistem mitigacije (inline) analizira dejanski promet in filtrira DDoS-promet.
- Legitimen promet se vrača nazaj v omrežje in proti naročniku.



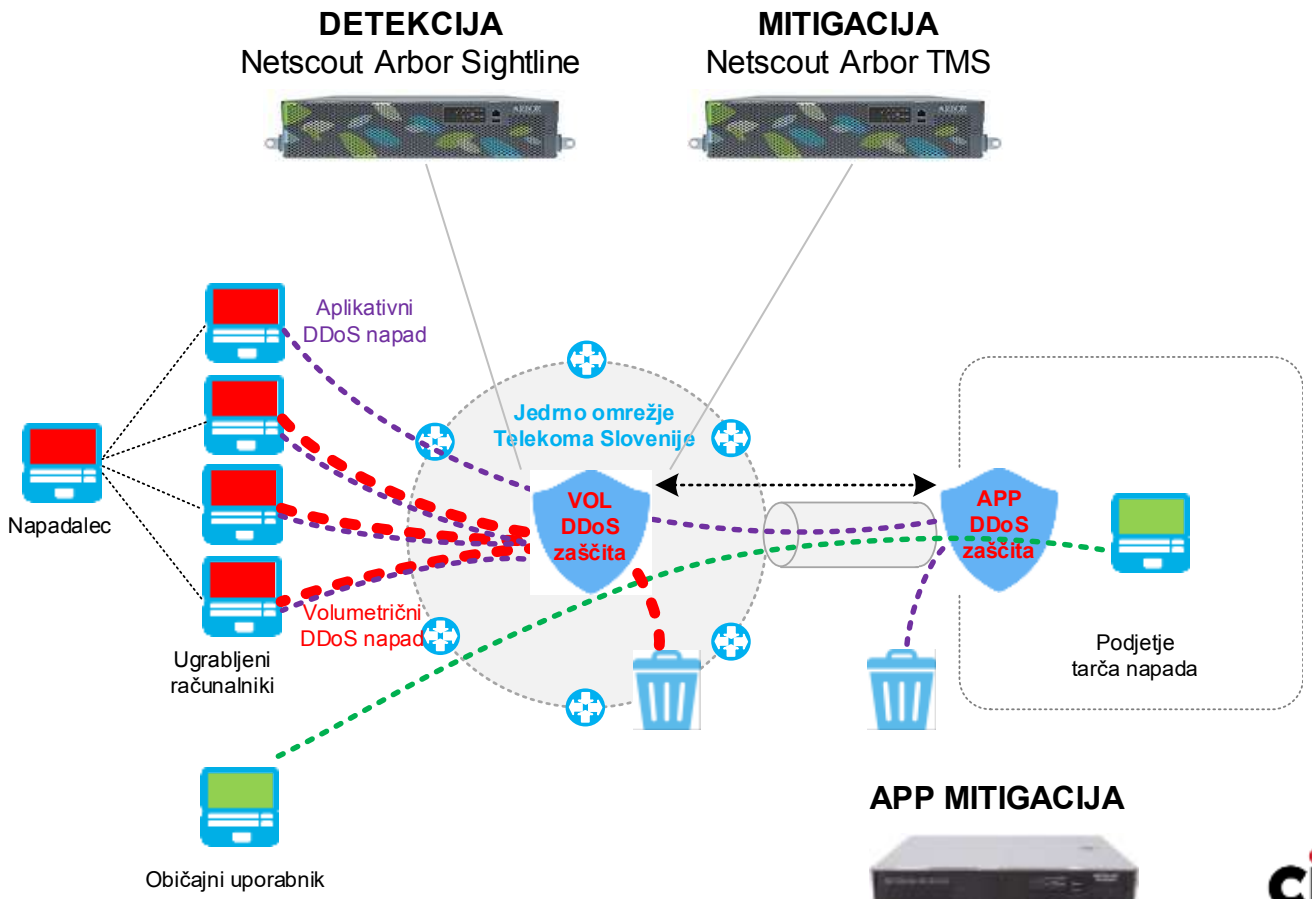
Zaščita v primeru velikih napadov

- Aktivira se blackhole ali flowspec mehanizem.
- Celotno omrežje postane sistem DDoS-mitigacije.
- Zaščita za 50-100 Gbps napade.

TelekomSlovenije

Zaščita pred aplikativnimi napadi DDoS

- Sistem AED je pri naročniku postavljen pred usmerjevalnik in FW in ščiti „statefull“ naprave.
- Sistem AED inline analizira ves promet (vhodni in izhodni) in takoj reagira na anomalije.
- Konfigurira se specifične nastavitve za posamezne storitve ali vrste naprav, ki jih ščiti.
- Promet se preverja na podlagi DDoS-statičnih in dinamičnih nastavitev ter glede na Atlas Inteligence Feed (AIF).



APP MITIGACIJA

Netscout Arbor Edge Defense

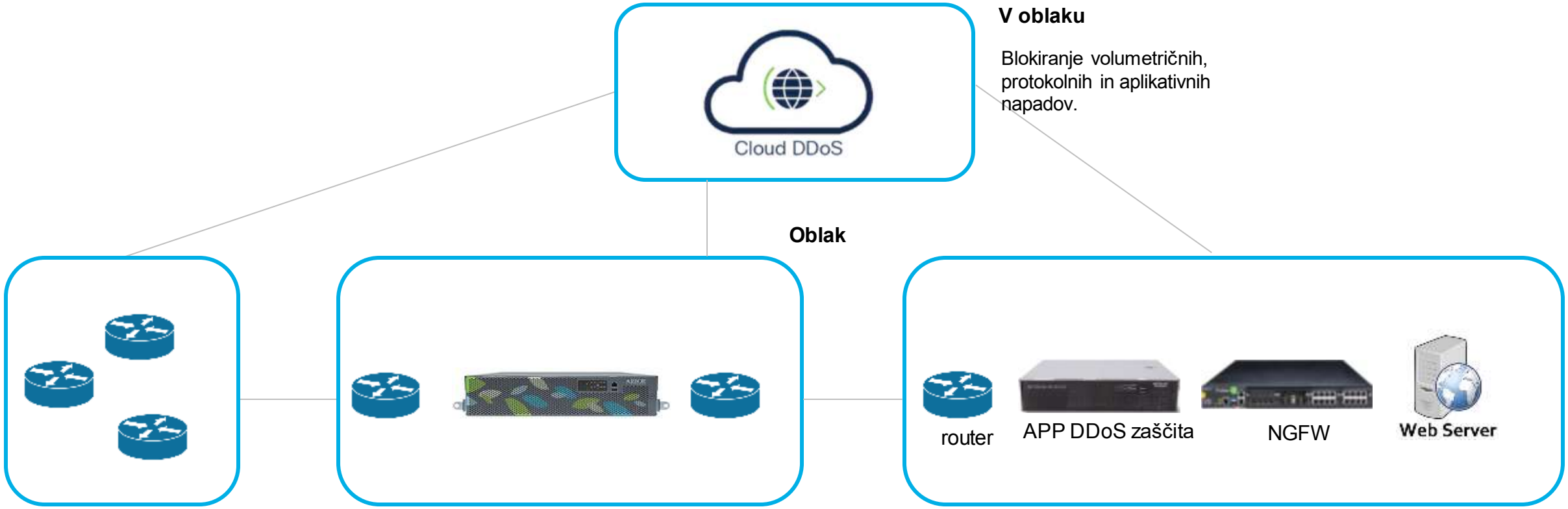
Radware DefensePro

CITRIX

Cloudflare DDoS Protection

TelekomSlovenije

Celostna zaščita pred napadi DDoS



V oblaku

Blokiranje volumetričnih, protokolnih in aplikativnih napadov.

Oblak

Globalni Internetni ponudnik

Blokiranje volumetričnih napadov velikega obsega

Lokalni Internetni ponudnik

Blokiranje volumetričnih, protokolnih in delno aplikativnih napadov.

Podjetje

Blokiranje protokolnih in aplikativnih napadov.
SSL dekripcija

TelekomSlovenije

Storitev DDoS-zaščite Telekoma Slovenije

Storitev	Osnovna DDoS zaščita	Standardna DDoS zaščita
Vključitev DDoS zaščite na internet dostopu/ih	X	X
Nastavitev priporočenih parametrov zaščite	X	X
Vpis kontakta za pošiljanje alarmov in mesečnih poročil	X	X
Avtomatsko pošiljanja mesečnih poročil	X	X
Avtomatski alarmi na e-mail	X	X
Prijave napak in dogodkov, odziv glede na možnosti (best effort)	X	
Prilagoditve parametrov DDoS zaščite, dodatni objekti posebej za naročnika		X
Prijave napak in dogodkov, odziv glede na SLA v VPI pogodbi		X
Dostop naročnika do DDoS sistema		X
Dodatni kontakti za alarme, poročila		X

Vključitev zaščite

- Kreiranje objekta (managed object) z IP omrežji.
- Določitev parametrov detekcije, privzete in opcijske nastavitve.
- Določitev parametrov mitigacije, privzete in opcijske nastavitve.

Pošiljanje alarmov, poročil

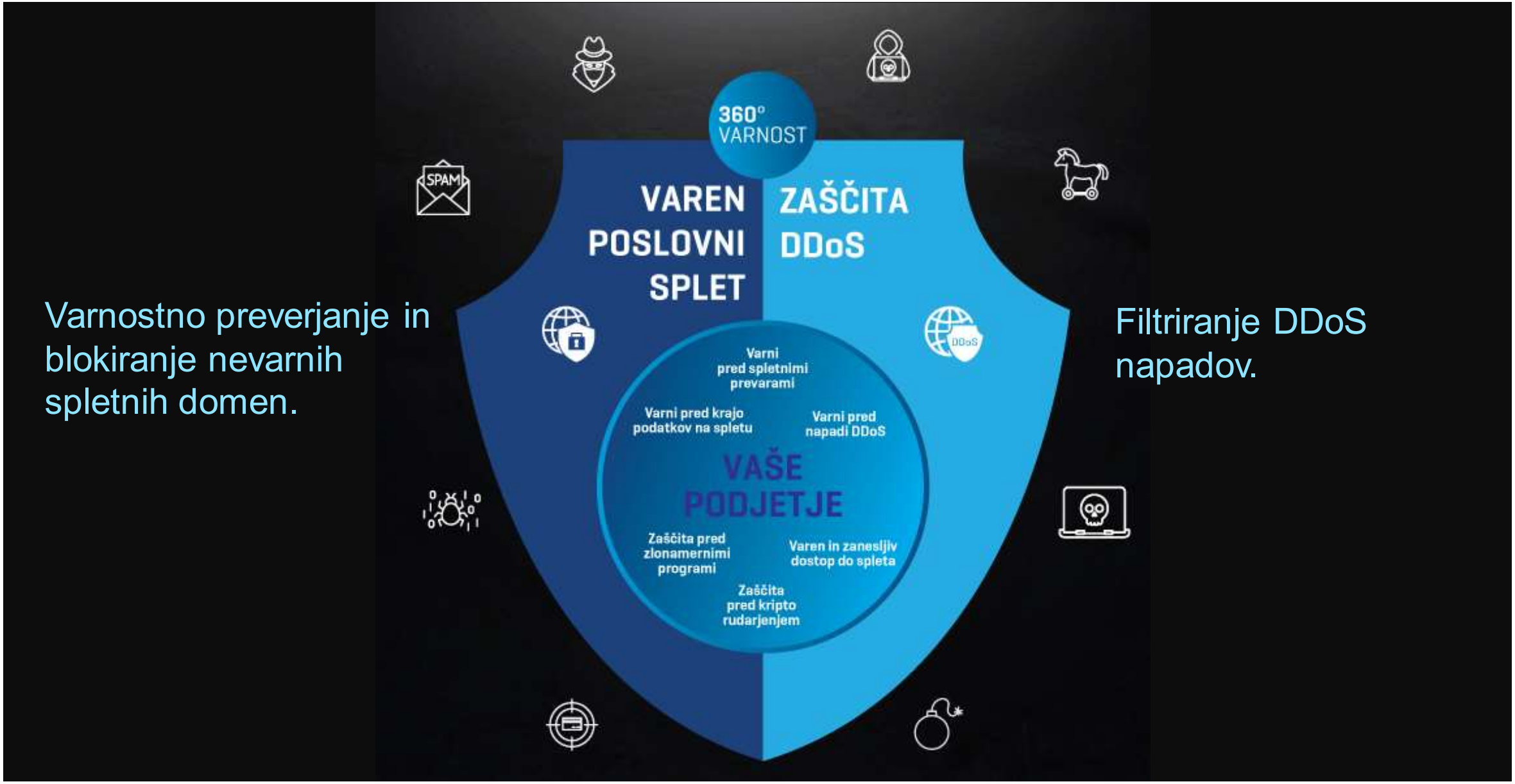
- Kreiranje skupin in pravil za obveščanje (notification group, notification rule), vpis kontaktnih e-naslovov.
- Kreiranje mesečnih poročil, ki se pošiljajo prek e-pošte

Dostop, prilagoditve (standard)

- Kreiranje uporabniških računov, vezano na javni IP-naslov naročnika.
- Pregled podrobnosti alarmov in mitigacij.
- Dodatni objekti za npr. www, prilagojena detekcija in mitigacija, podpora med napadi

Osnovna zaščita za vsako podjetje - Varen poslovni splet in DDoS

Varnostno preverjanje in blokiranje nevarnih spletnih domen.



Filtriranje DDoS napadov.

TelekomSlovenije

Hvala.

Telekom Slovenije, d.d.
Cigaletova 15
1000 Ljubljana

www.telekom.si
E: info@telekom.si

facebook.com/TelekomSlovenije

@TelekomSlo

youtube.com/TelekomSlovenije

@telekom_slovenije

WEBINAR JE OMOGOČILA:

zit SeKV

Združenje za informatiko in telekomunikacije
Kibernetska varnost

TelekomSlovenije

KIBERNETSKI CUNAMI:

Uničujoča moč DDoS napadov

Zoom platforma, 6. junij 2024

zit SeKV
Združenje za informatiko in telekomunikacije
Kibernetska varnost

Gospodarska zbornica Slovenije

zit Združenje za informatiko in telekomunikacije

SRIP GoDigital

Sofinancira Evropska unija

I FEEL SLOVENIA

„Naložbo sofinancira Evropska unija iz Evropskega sklada za regionalni razvoj“

HVALA ZA UDELEŽBO!

Za dodatna vprašanja smo dosegljivi na:
sekv@gzs.si

zit SeKV
Združenje za informatiko in telekomunikacije
Kibernetska varnost

Gospodarska zbornica Slovenije

zit Združenje za informatiko in telekomunikacije

SRIP GoDigital

Sofinancira Evropska unija

I FEEL SLOVENIA

„Naložbo sofinancira Evropska unija iz Evropskega sklada za regionalni razvoj“