

Priložnosti in (ne)varnosti digitalizacije



Sašo Žbontar

saso.zbontar@telekom.si

Metod Platiše

metod.platise@telekom.si

CISCOSEC

Živimo v digitalnem svetu

Se zavedamo?

Smo pripravljeni ?



Nevarnosti digitalnega sveta

- Ranljivost sistema
- Najšibkejši člen
- Virusi
- Črvi
- Trojanski konji
- Bootnets
- Izsiljevalski SW “Pay or else ...“
- DoS, DDoS ...

Se znamo zavarovati ?

- Aktivna/pasivna varnost
- Obvezno zavarovanje
- Kasko zavarovanje
- Požarne pregrade
- ...

avto, nepremičnine
življenje, zdravje
informacije

Kadyrovtsy



ezBTC Squad



RedDoor



Locky
Samas
Petya
Cerber
BART
CTB Locker
CryptXXX
Unlock 92
TeslaCrypt
Jigsaw

Vseobsegajoča varnost

Varnostna utrditev funkcionalnih elementov IKT (implicitna varnost)



Varnostni sistemi in storitve (eksplicitna varnost)



Ključna vprašanja

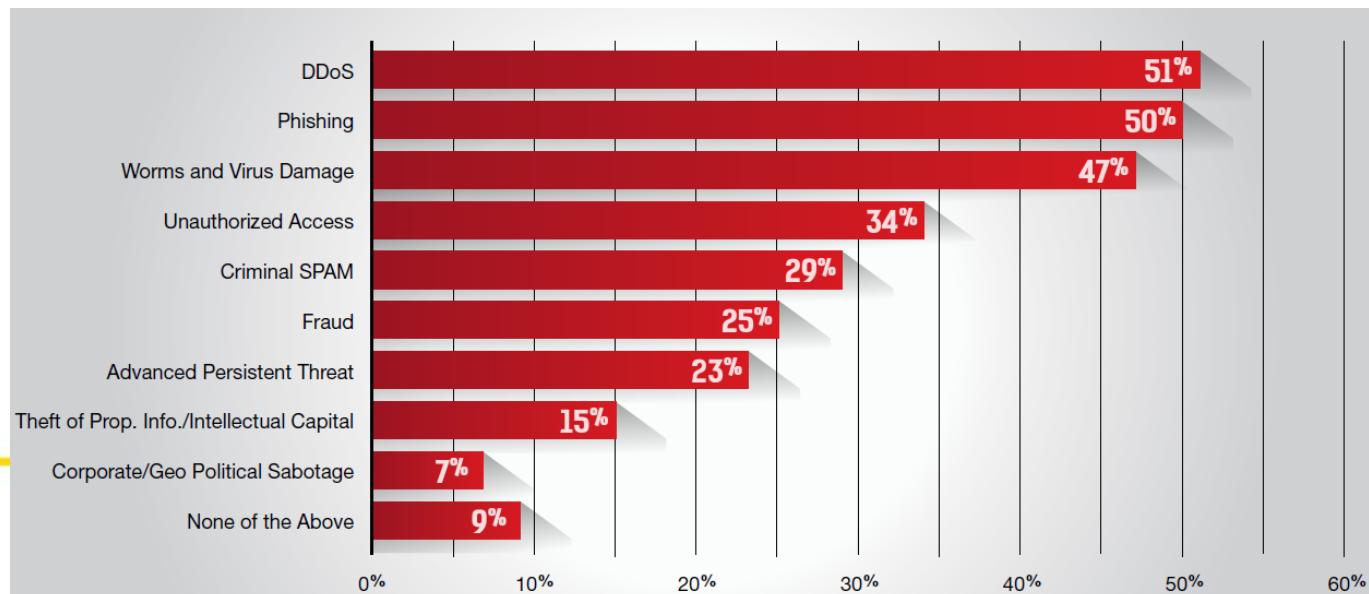
- Smo že bili napadeni, ne še...kdaj bomo ?
- Ali smo pripravljeni na kibernetsko izsiljevanje ? Bomo plačali ?
- Ali bomo javno komunicirali, prijavljali organom ?
- Ali imamo tehnične vire za obvladovanje situacij?
- Ali smo zavarovani v primeru poslovne izgube ?
- Ali imamo načrt za obvladovanje varnostnih tveganj ?
- Ali imamo operativni plan za odzivanje na takšne dogodke?
- Ali imamo načrt okrevanja ?
-



DoS/DDoS ali onemogočanje

Napad onemogočanja je poskus da se onemogoči delovanje IKT storitve.
Večinoma so napadi usmerjeni na spletne storitve.

Onemogočanje je lahko samostojen napad, lahko je krinka za globlji vdor.
Napad je lahko bolj ali manj agresiven, lahko traja poljubno dolgo.



vir: Radware 2015-2016 Global Application And Network Security Report

Več kot 90% organizacij je že doživelo kibernetski napad.

Več kot 51 organizacij % je doživelo napad onemogočanja ki je tudi najbolj pogost napad.*

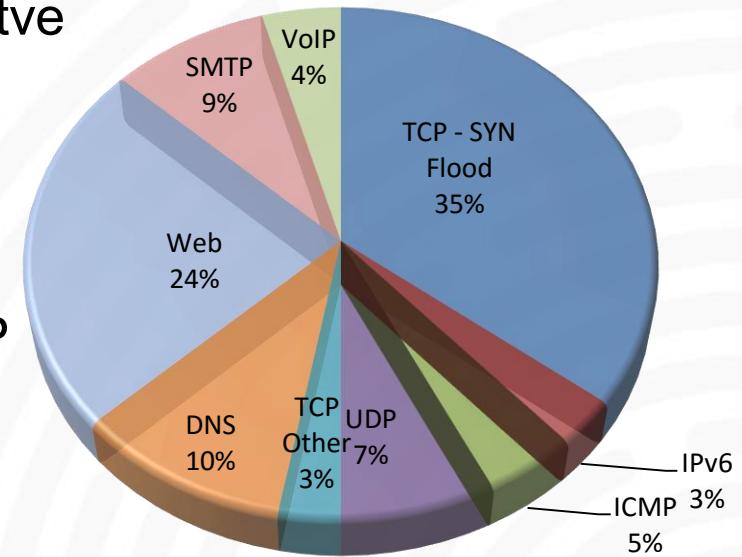
Tipi napadov onemogočanje

Volumetrični napad zapolni pasovno širino povezave storitve do Internet omežja in običajnim uporabnikom onemogoči dostop do storitve

Napad z velikim številom TCP povezav je usmerjen na naprave ki si zapomnijo stanja povezav, jim s tem zapolni RAM.

Napad s fragmentiranimi paketi je sestavljen iz velike množice TCP ali UDP fragmentov, ki jih napadena naprava poskuša sestavljati, pri tem porablja procesorske zmogljivosti.

Aplikativni napad je usmerjen na določeno storitev in izkorišča njeno funkcionalnost ali pomanjkljivost, običajno ne potrebuje velike količine prometa, je specifičen in ga je zato težje odkriti in preprečiti.



Vir: Radware Security Report

Proženje napadov onemogočanje

Priprava okolja za napad na način, da napadalci okužijo veliko število naprav v Internetu s programi (boti), ki jim omogočijo, da prevzamejo kontrolo nad napravo.

Proženje napada z aktiviranjem okuženih naprav in z uporabo določene ali kombinacije metod onemogočanja in usmeritvijo napada na izbrano internetno storitev.

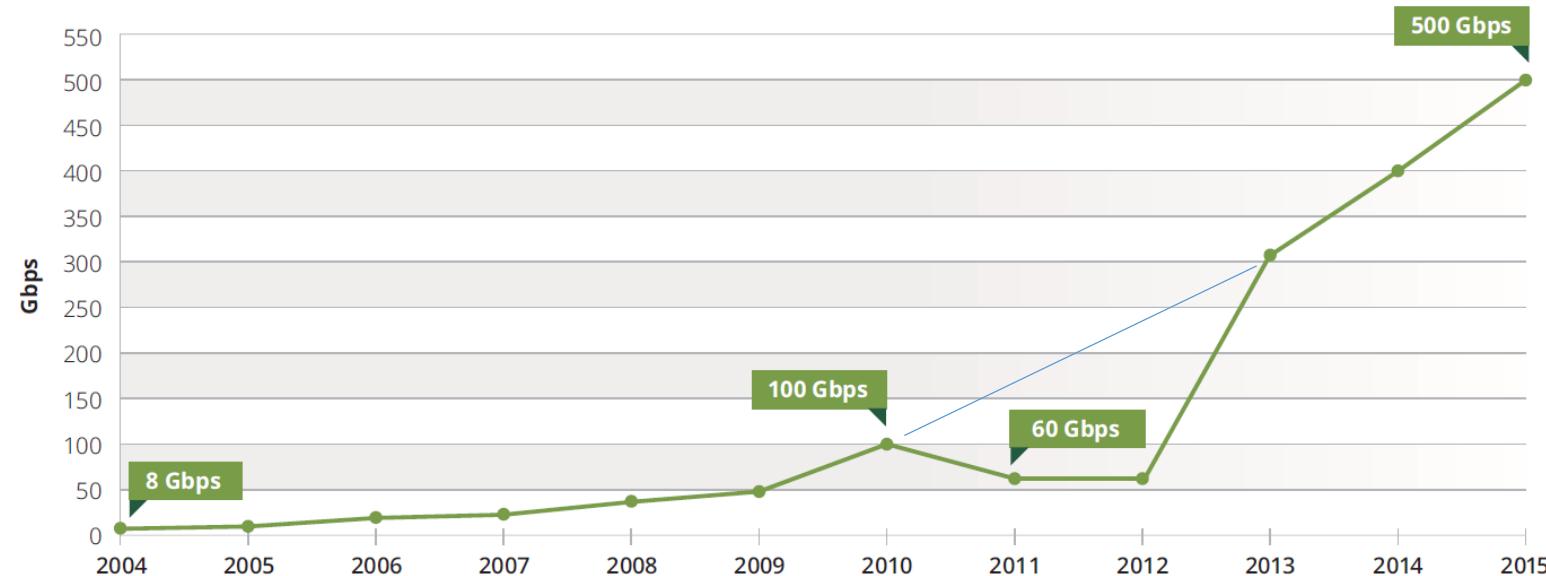
Pri napadih z odbojem in ojačanjem je lahko za ojačanje učinka uporabljena legitimna infrastruktura (DNS reflection, Chargen reflection, smurf napad,...)



Onemogočanje kot storitev (DDoSaaS) je velik posel, za 10EUR se dobi „spodoben“ napad.
Napadalcem ne plačujte !
ker jih s tem financirate

Rast volumetričnih napadov

Največji registrirani volumetrični napadi po letih.*



V TS največji zabeleženi napad je bil na hčerinsko firmo v velikosti 23Gbps.

* vir: Arbor Networks Worldwide Infrastructure Security Report

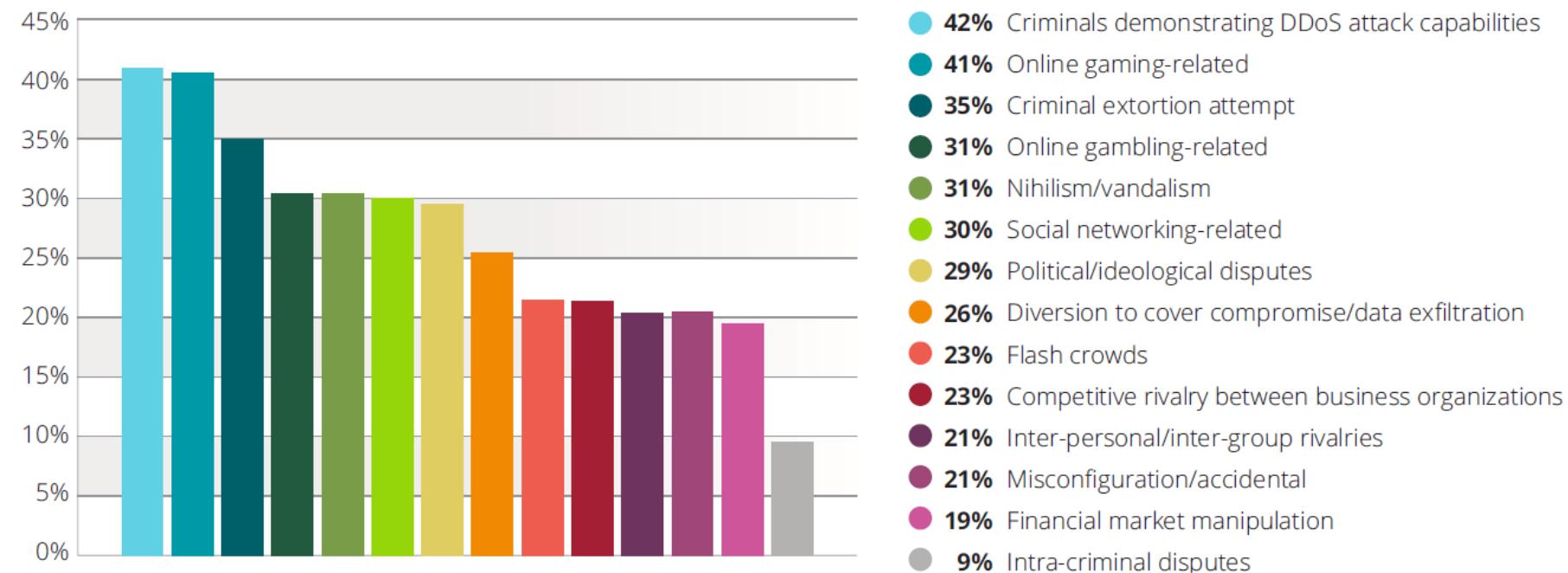
Skoraj tri četrtine operaterjev globalno ima sredstva, da lahko prepreči napad onemogočanja *

Med njimi je tudi Telekom Slovenije

Motivi onemogočanja

Motiv napada je lahko materialna korist, onemogočanje konkurence, (hackt)ivizem, objestnost, politično motivirano...

Kibernetski kriminal je vreden 0,8% BDP globalno (droge 0,9%)*



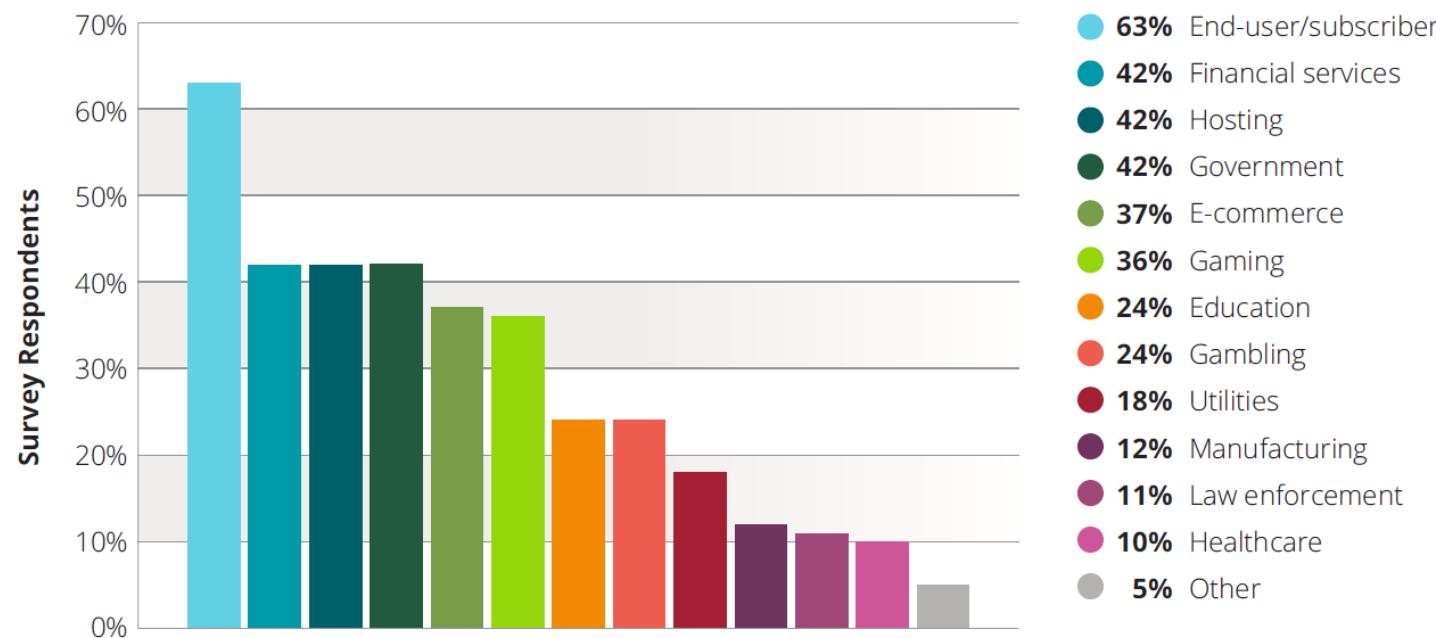
Slovenski kibernetski napadalci so predstavljeni v filmu #hekerji.si priporočam ogled

* vir: McAfee and the center for strategic and international studies, 2014

** vir: Arbor Networks Worldwide Infrastructure Security Report

Žrtve onemogočanja

Žrtve napadov onemogočanja z vidika ponudnikov storitev.



* vir: Arbor Networks Worldwide Infrastructure Security Report

Kaj se ta trenutek dogaja na globalni DDoS sceni ?

Digital Attack Map

<http://www.digitalattackmap.com>

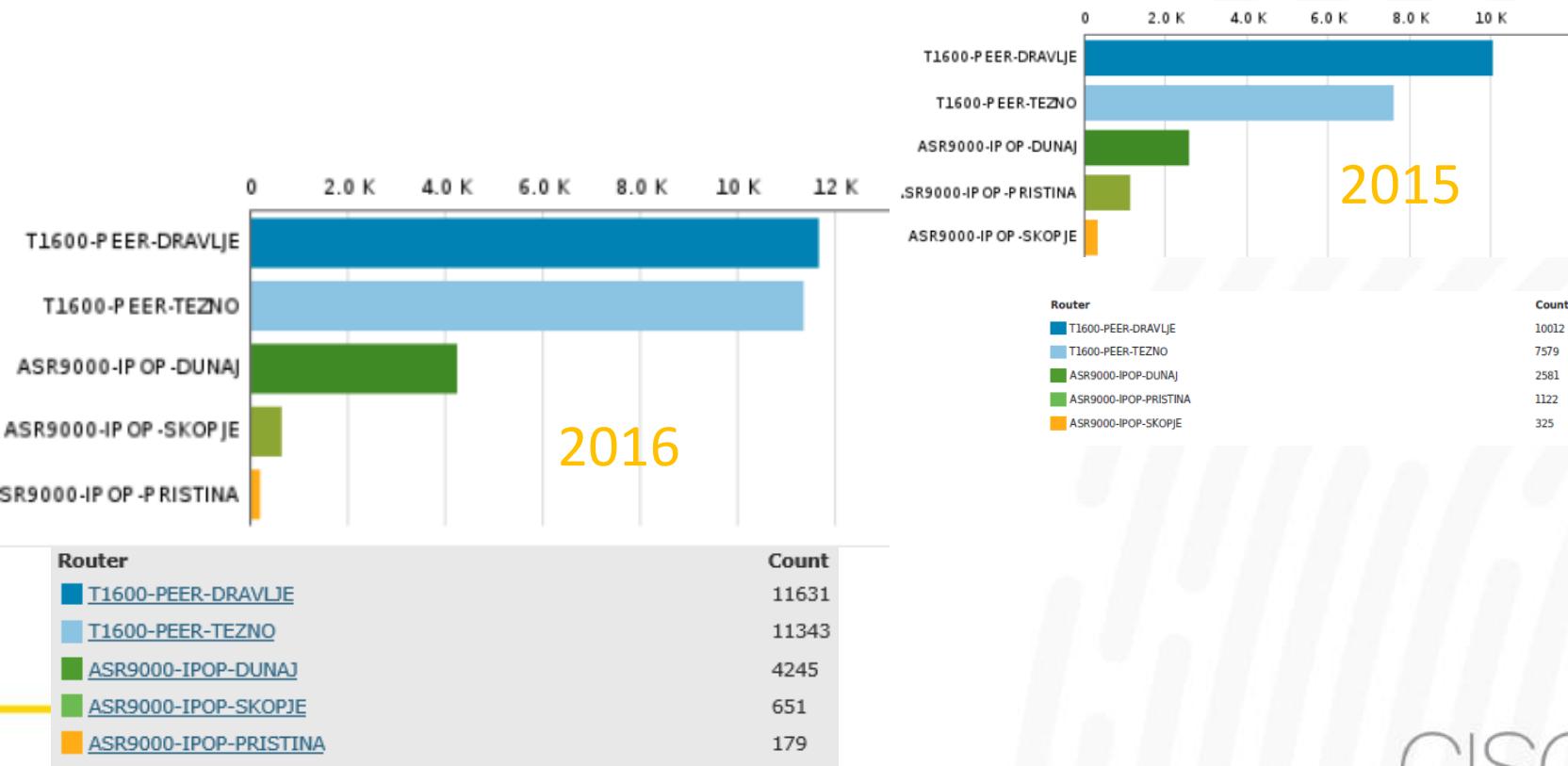
DDoS napadi v omrežju TS

- Graf prikazuje distribucijo DDoS napadov zabeleženih v omrežju TS glede na resnost napada



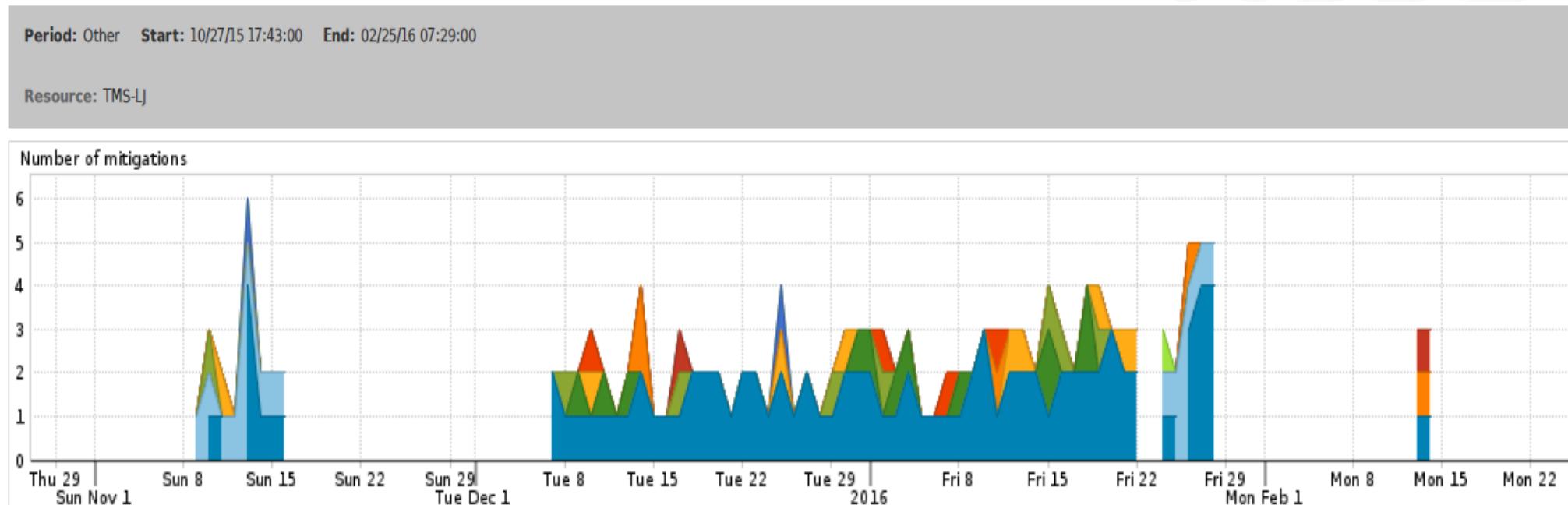
DDoS v omrežju TS

- Porazdelitev napadov glede na opazovane točke v omrežju TS



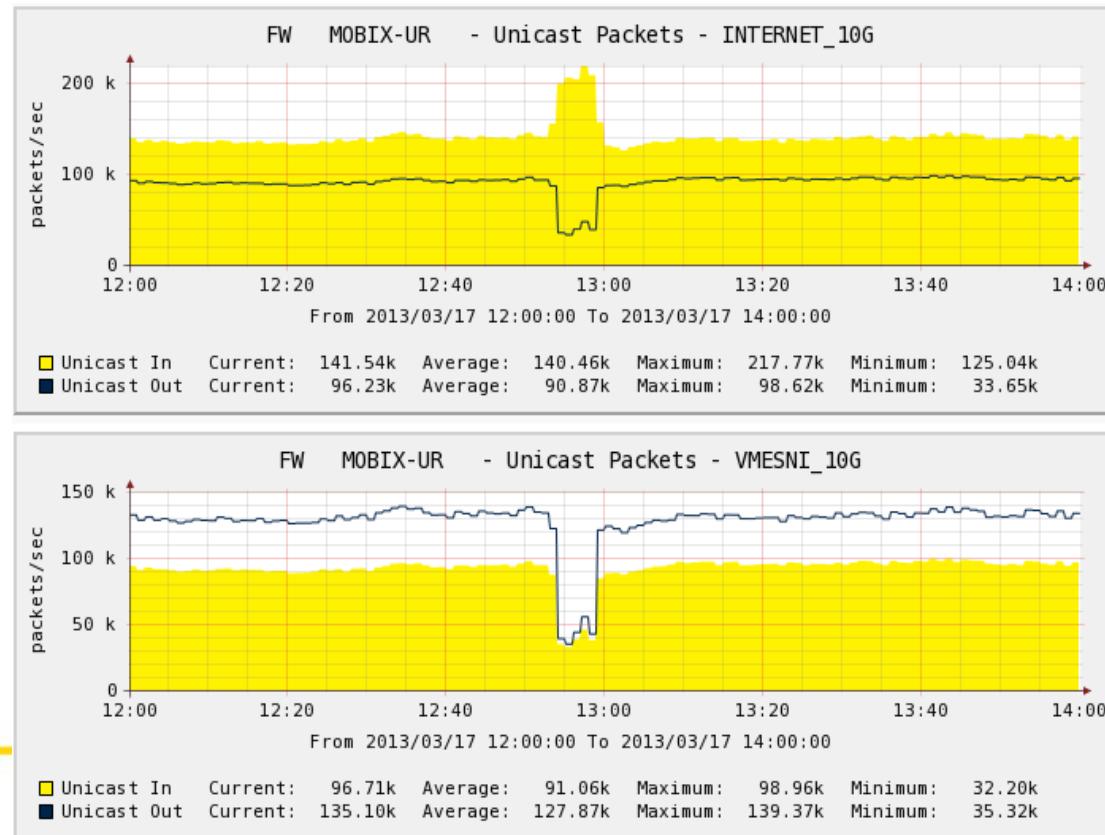
DDoS v omrežju TS

- Število mitigacij zabeleženih v omrežju TS (november-februar)



DDoS v omrežju TS

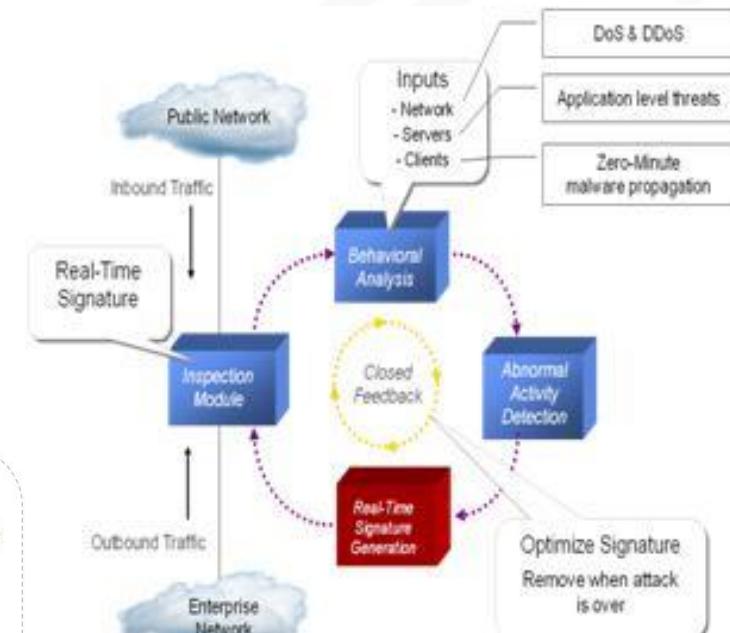
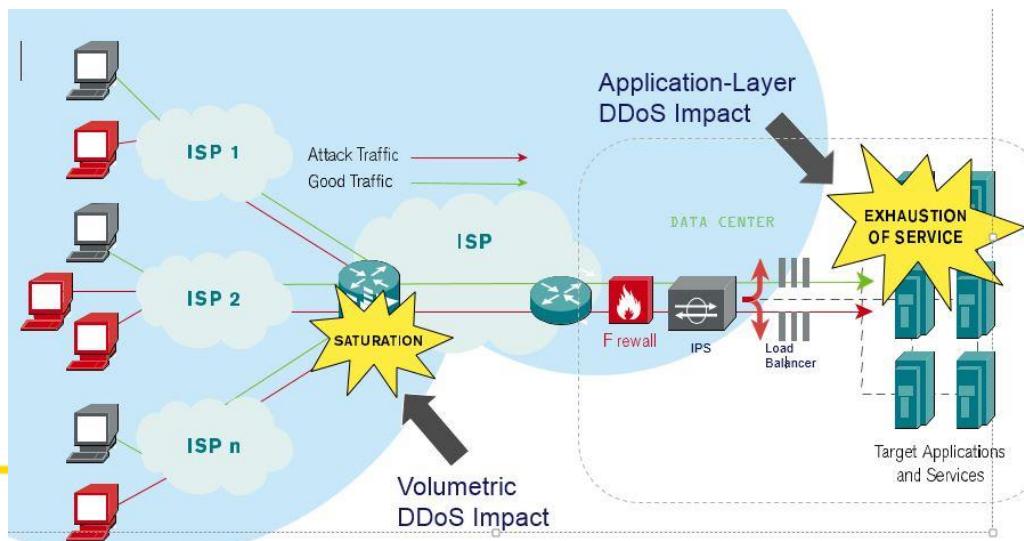
- Primer DDoS napada zabeleženega v omrežju TS
- Na grafu vidimo kako povečano število paketov vpliva na prepustnost požarnega zidu



Vir: Interni podatki TS

Obramba proti DDoS v TS

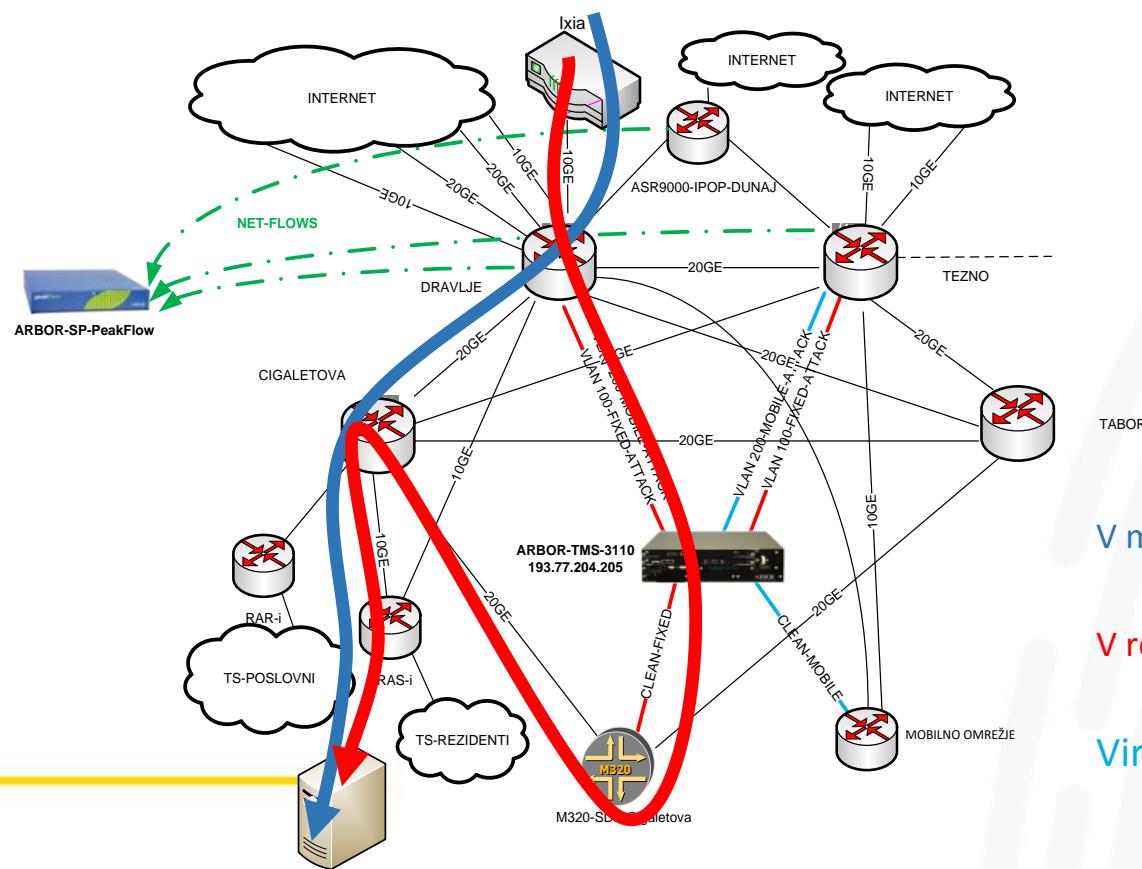
- Slika prikazuje način obrambe proti DDoS
 - Analiza -> Detekcija -> Izločanje lažnega IP prometa



Vir: Radware

Obramba proti DDoS v TS

- Na sliki je prikazana omrežna infrastruktura, ki v TS omogoča čiščenje zlonamernega IP prometa



V modri barvi je prikazan običajni prometni tok

V rdeči barvi – tok prometa v primeru čiščenja

Vir: Telekom Slovenije, d.d.

Primer napada DDoS

Duration: Feb 23 17:17 – 17:25 (0:08)

Mitigations

TMS:

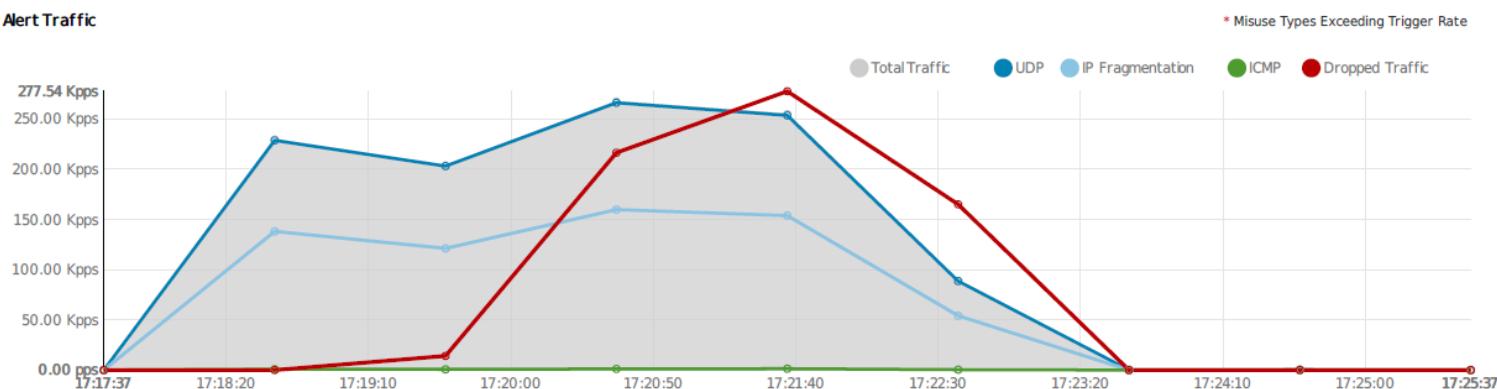
Name	Dropped	Passed
Alert 966184 Auto-Mitigation	N/A	N/A

Period: Alert Timeframe Units: pps View: Network Boundary

Summary

Severity Level: High Impact: 2.8 Gbps/298.2 Kpps Direction: Incoming Misuse Types: Total Traffic Managed Object: Mobitel Subscribers Target: 213.229.198.52
⚠️ Fast Flood Top Misuse Type: **Total Traffic** at Managed Object Boundary

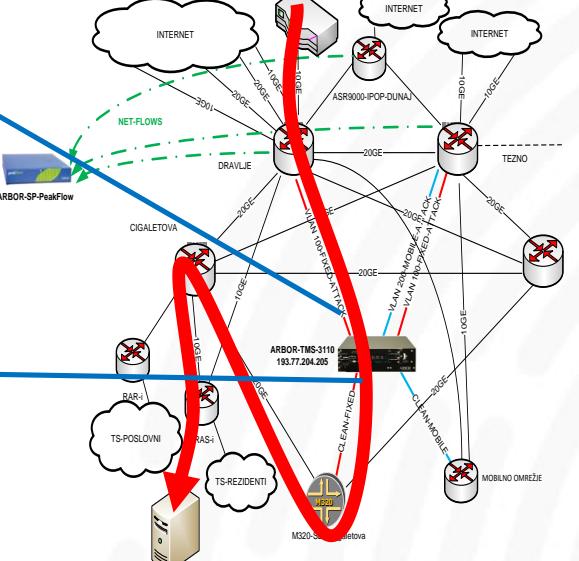
Alert Traffic



Top Traffic Patterns (last 5 minutes)

Source	Protocol	Flags	Src Port	Destination	Dest Port	Router	Alert Traffic
1. Highly Distributed	UDP	--	0	213.229.198.52/32	0	T1600-PEER-TEZNO	106.80 Kpps
2. Highly Distributed	UDP	--	19 (chargen)	213.229.198.52/32	1024 - 65535 (Dynamic)	T1600-PEER-TEZNO	73.20 Kpps
3. Highly Distributed	UDP	--	0	213.229.198.52/32	0	T1600-PEER-DRAVLJE	45.60 Kpps
4. Highly Distributed	UDP	--	19 (chargen)	213.229.198.52/32	1024 - 65535 (Dynamic)	T1600-PEER-DRAVLJE	30.93 Kpps
5. 146.66.155.122/32	UDP	--	27067	213.229.198.52/32	27005	T1600-PEER-TEZNO	200.00 pps
6. 185.62.190.176/32	UDP	--	9984	213.229.198.52/32	56366	T1600-PEER-TEZNO	133.00 pps
7. 188.75.70.126/32	UDP	--	19 (chargen)	213.229.198.52/32	4142 (oidocsvc)	T1600-PEER-TEZNO	66.00 pps
8. 89.19.14.178/32	UDP	--	0	213.229.198.52/32	0	T1600-PEER-TEZNO	66.00 pps
9. 31.13.84.8/32	TCP	AP	443 (https)	213.229.198.52/32	36420	T1600-PEER-TEZNO	66.00 pps

Obramba proti DDoS v TS



CISCO SEC

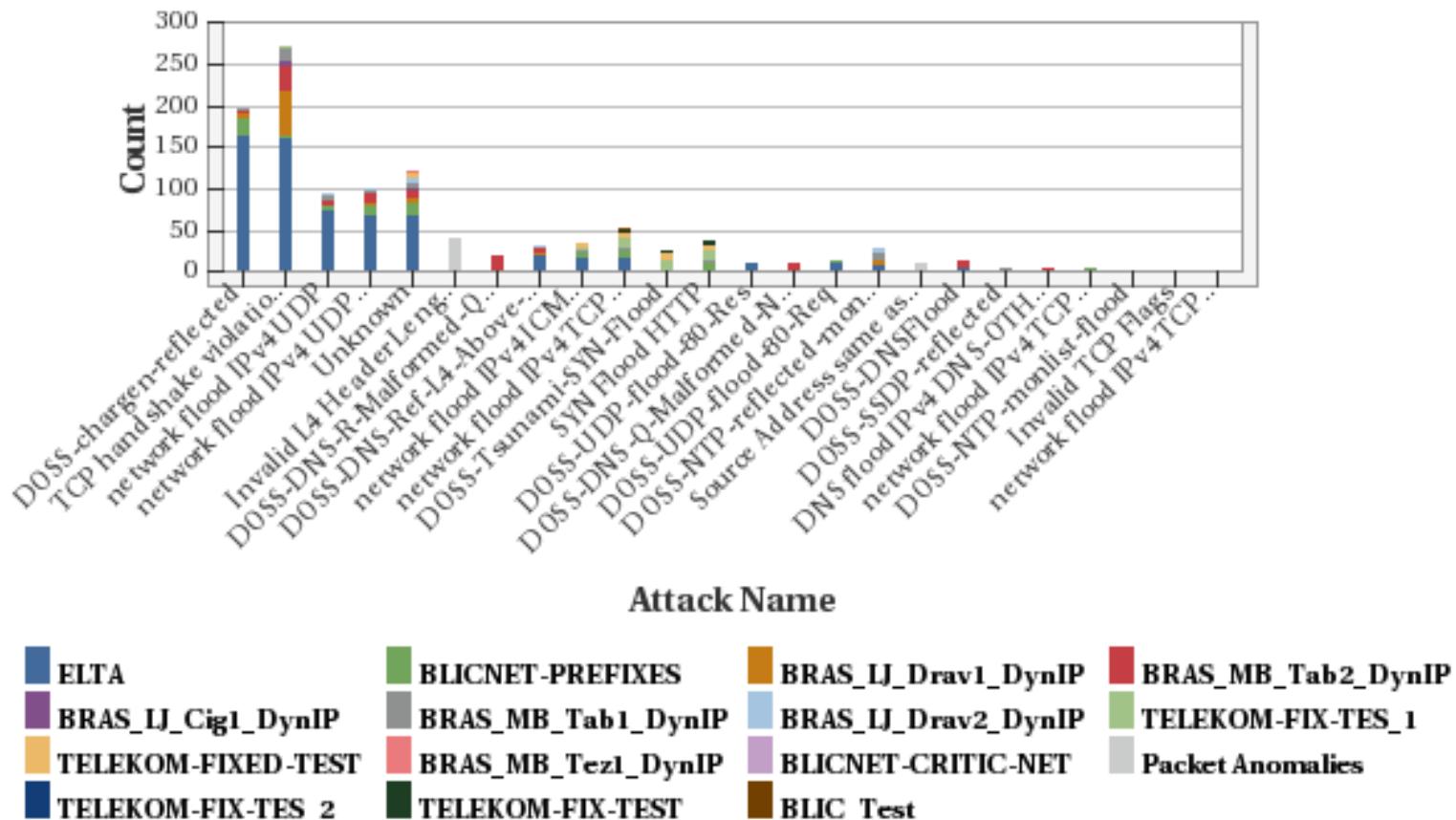
Vir: Telekom Slovenije, d.d.

Obramba proti DDoS v TS



- Pogostnost napadov posameznega tipa

Graph : Top Attacks



Vir: Telekom Slovenije, d.d.

CISCO SEC

Obramba proti DDoS v TS

Peakflow™

Peakflow SP: Customer Alerts

Thu 10 Nov 2016 14:54:48 CET



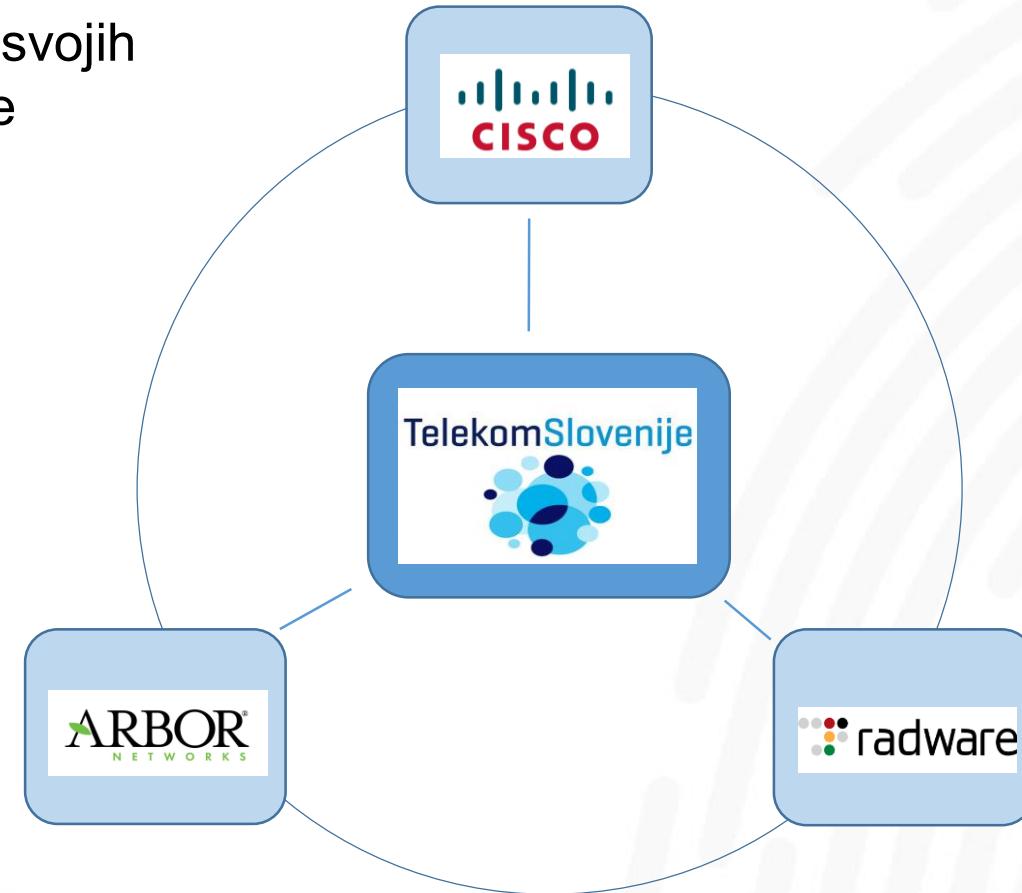
Period: This Year Start: 52 weeks ago End: now					
Customer: ELTA Description: ELTA CABLE PREFIXES					
ID	Graph	Importance ▾	Alert	Start Time	Classification & Annotations
1138575		High ⚡ Fast Flood 7.163.0% of 10 Kpps 11.9 Gbps, 11 Mpps	DoS Host Alert Incoming Host Alert to 31.47.11.1 using ELTA Misuse Types: IP Fragmentation, Total Traffic, UDP, DNS Amplification	Oct 27 12:34 – 12:37 (0:03)	Possible Attack The "UDP" host alert signature has been triggered at router "T1600-PEER-DRAVLJE". (expected rate: 300.00 Kpps, observed rate: 811.86 Kpps) (by auto-annotation)
1100446		High 4.274.0% of 10 Kpps 6.8 Gbps, 651.4 Kpps	DoS Host Alert Incoming Host Alert to 217.71.53.176 using ELTA Misuse Types: ICMP, IP Fragmentation, Total Traffic, UDP, DNS Amplification	Sep 17 20:17 – 20:36 (0:19)	Possible Attack The "UDP" host alert signature has been triggered at router "T1600-PEER-DRAVLJE". (expected rate: 300.00 Kpps, observed rate: 325.61 Kpps) (by auto-annotation)
1146224		High ⚡ Fast Flood 3.424.0% of 10 Kpps 5.5 Gbps, 534.0 Kpps	DoS Host Alert Incoming Host Alert to 62.68.111.91 using ELTA Misuse Types: IP Fragmentation, Total Traffic, UDP, DNS Amplification	Nov 6 13:21 – 13:29 (0:08)	Possible Attack The "UDP" host alert signature has been triggered at router "T1600-PEER-DRAVLJE". (expected rate: 300.00 Kpps, observed rate: 412.76 Kpps) (by auto-annotation)
1103069		High ⚡ Fast Flood 2.512.0% of 10 Kpps 4.1 Gbps, 403.4 Kpps	DoS Host Alert Incoming Host Alert to 188.124.213.82 using ELTA Misuse Types: ICMP, IP Fragmentation, Total Traffic, UDP, DNS Amplification	Sep 20 21:55 – 21:59 (0:04)	Possible Attack The "ICMP" host alert signature has been triggered at router "ASR9000-POP-PRISTNA". (expected rate: 2.50 Kpps, observed rate: 2.67 Kpps) (by auto-annotation)
1103063		High ⚡ Fast Flood 2.226.0% of 10 Kpps 3.7 Gbps, 361.0 Kpps	DoS Host Alert Incoming Host Alert to 188.124.213.82 using ELTA Misuse Types: ICMP, IP Fragmentation, Total Traffic, DNS Amplification	Sep 20 21:41 – 21:50 (0:09)	Possible Attack The "ICMP" host alert signature has been triggered at router "ASR9000-POP-PRISTNA". (expected rate: 2.50 Kpps, observed rate: 2.94 Kpps) (by auto-annotation)
1113836		High ⚡ Fast Flood 1.293.0% of 10 Kpps 1.9 Gbps, 209.4 Kpps	DoS Host Alert Incoming Host Alert to 31.47.15.182 using ELTA Misuse Types: IP Fragmentation, Total Traffic, charge Amplification	Oct 2 19:04 – 19:10 (0:07)	Possible Attack The "charge Amplification" host alert signature has been triggered at router "T1600-PEER-DRAVLJE". (expected rate: 200.00 Mbps/30.00 Kpps, observed rate: 338.53 Mbps/31.60 Kpps) (by auto-annotation)
1145722		High ⚡ Fast Flood 824.0% of 10 Kpps 1.3 Gbps, 126.0 Kpps	DoS Host Alert Incoming Host Alert to 62.68.104.128 using ELTA Misuse Types: IP Fragmentation, Total Traffic, DNS Amplification	Nov 5 20:54 – 22:20 (1:26)	Possible Attack The "DNS Amplification" host alert signature has been triggered at router "T1600-PEER-DRAVLJE". (expected rate: 200.00 Mbps/30.00 Kpps, observed rate: 269.43 Mbps/23.85 Kpps) (by auto-annotation)
1099550		High 782.0% of 10 Kpps 862.5 Mbps, 85.0 Kpps	DoS Host Alert Incoming Host Alert to 31.47.14.244 using ELTA Misuse Types: IP Fragmentation, Total Traffic	Sep 16 21:33 – 21:38 (0:05)	Possible Attack The "IP Fragmentation" host alert signature severity rate configured for "ELTA" has been exceeded for 3 minutes, changing Severity Level from medium to high (expected rate: 10.00 Kpps, observed rate: 78.16 Kpps) (by auto-annotation)
1103797		High 749.0% of 10 Kpps 1.0 Gbps, 104.8 Kpps	DoS Host Alert Incoming Host Alert to 79.143.162.246 using ELTA Misuse Types: IP Fragmentation, Total Traffic	Sep 21 18:24 – 18:31 (0:07)	Possible Attack The "IP Fragmentation" host alert signature severity rate configured for "ELTA" has been exceeded for 3 minutes, changing Severity Level from medium to high (expected rate: 10.00 Kpps, observed rate: 74.93 Kpps) (boundary: managed object) (by auto-annotation)
1142501		High ⚡ Fast Flood 617.0% of 600 Mbps 3.7 Gbps, 11 Mpps	DoS Host Alert Incoming Host Alert to 31.47.1.164 using ELTA Misuse Types: Total Traffic, UDP, SSDP Amplification	Nov 1 21:33 – 22:36 (1:03)	Possible Attack The "SSDP Amplification" host alert signature has been triggered at router "T1600-PEER-DRAVLJE". (expected rate: 200.00 Mbps/100.00 Kpps, observed rate: 277.07 Mbps/106.17 Kbps) (by auto-annotation)
1116512		High ⚡ Fast Flood 535.0% of 10 Kpps 595.7 Mbps, 59.1 Kpps	DoS Host Alert Incoming Host Alert to 31.47.1.16 using ELTA Misuse Types: IP Fragmentation, Total Traffic	Oct 4 20:25 – 20:29 (0:04)	Possible Attack The "Total Traffic" host alert signature has been triggered at router "T1600-PEER-DRAVLJE". (expected rate: 300.00 Mbps/300.00 Kpps, observed rate: 350.44 Mbps/34.21 Kbps) (by auto-annotation)
1119118		High 472.0% of 10 Kpps 591.0 Mbps, 78.8 Kpps	DoS Host Alert Incoming Host Alert to 79.143.160.12 using ELTA Misuse Types: IP Fragmentation, Total Traffic	Oct 7 19:11 – 19:19 (0:08)	Possible Attack The "Total Traffic" host alert signature has been triggered at router "T1600-PEER-DRAVLJE". (expected rate: 300.00 Mbps/300.00 Kpps, observed rate: 471.89 Mbps/63.12 Kbps) (by auto-annotation)
1119154		High 471.0% of 10 Kpps 950.2 Mbps, 109.4 Kpps	DoS Host Alert Incoming Host Alert to 79.143.160.12 using ELTA Misuse Types: IP Fragmentation, Total Traffic	Oct 7 20:02 – 20:13 (0:11)	Possible Attack The "IP Fragmentation" host alert signature severity rate configured for "ELTA" has been exceeded for 3 minutes, changing Severity Level from medium to high (expected rate: 10.00 Kpps, observed rate: 44.24 Kpps) (boundary:

CISCO SEC

Partnerstvo v DDoS zaščiti



V Telekomu Slovenije za zaščito svojih naročnikov uporabljamo najboljše razpoložljive tehnologije



CISCOSEC

Ponudba storitev v TS – čiščenje DDoS

Telekom Slovenije v okviru naprednih storitev ponuja naslednje:

- Osnovni paket

- mesečna naročnina
- ni avtomatske detekcije napadov
- ni avtomatskega čiščenja napadov
- obračunava se vsako čiščenje napada, ki ga stranka sproži s klicem na Telekom Slovenije
- mesečno poročilo

- Nadstandardni paket

- mesečna naročnina
- avtomatska detekcija napadov
- avtomatsko čiščenje napadov
- mesečno poročilo





Hvala

Telekom Slovenije, d.d.

Cigaletova 15

1000 Ljubljana

www.telekom.si

T: 041 700 700 ali 080 8000

E: info@telekom.si

CISCO SEC