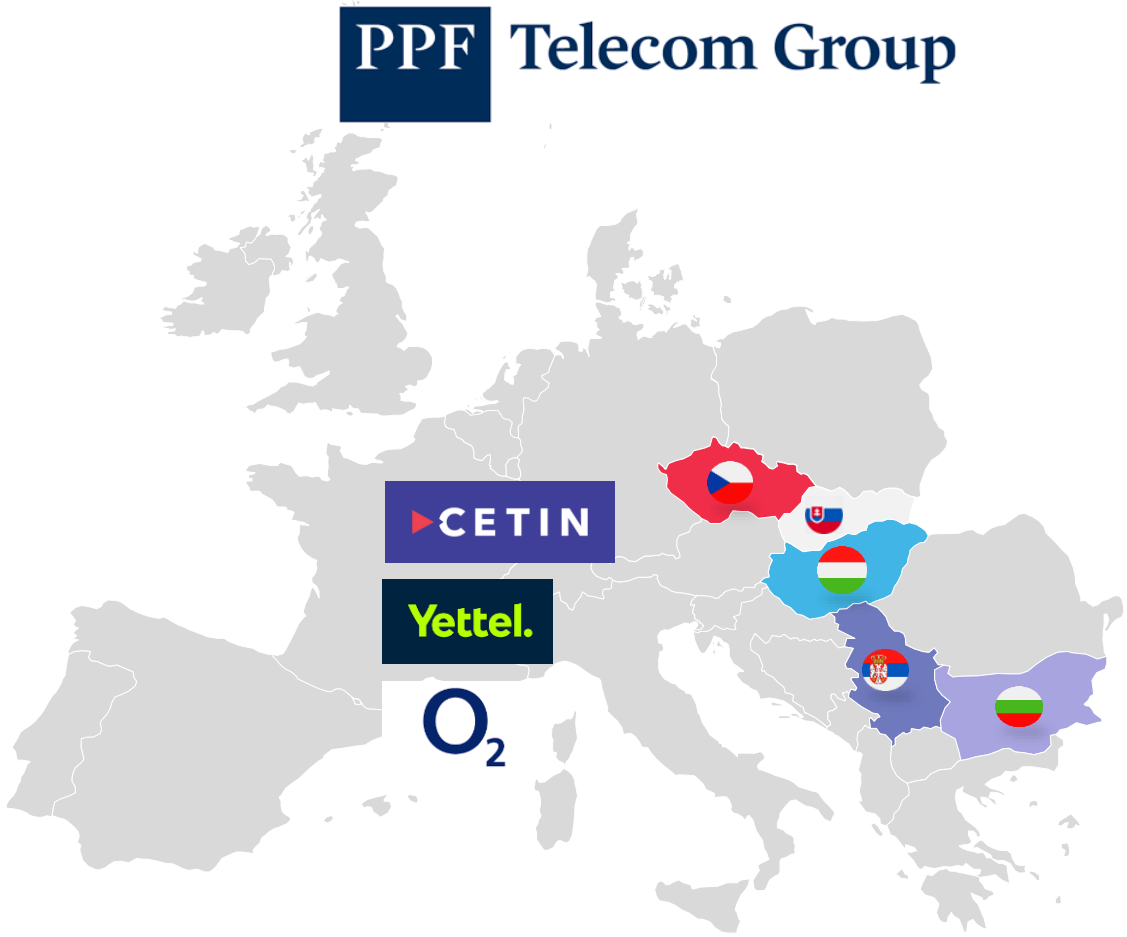
Kako zaštititi mrežu? Pametno praćenje i fina podešavanja

CETIN doo Beograd
Predrag Škundrić, Arhitekta za bezbednost

CETIN
MEMBER OF PPF GROUP

CETIN štiti 2,5 miliona krajnjih korisnika i 10 miliona uređaja na internetu

- Preko 20 godina ekspertize u izgradnji i upravljanju sigurnom mobilnom i fiksnom mrežom
- 5 data centara, preko 8500km optičke infrastrukture preko 2400 radio baznih stanica i preko 2700 parova radio relejnih predajnika
- Usluge: mreže, sajber bezbednosti, konektivnosti i upravljanje sistemima
- Domaći i strani klijenti
- ISO: 9001, 22301, 27001, 27701, 14001



CETIN
MEMBER OF PPF GROUP

Sadržaj

- **CETIN SOC dizajn**
- **CETIN SOC Analitika u 2023.**
  - DDoS napadi
  - Phishing
  - Malware
- **Primer maliciozne aktivnosti u praksi**
- **Šta smo zaključili?**

CETIN ima najviši nivo SOC-a

Nivo 1

Monitoring
Otvaranje tiketa i zatvaranje false positive nalaza
Osnovna istraga i ublažavanje uticaja

Nivo 2

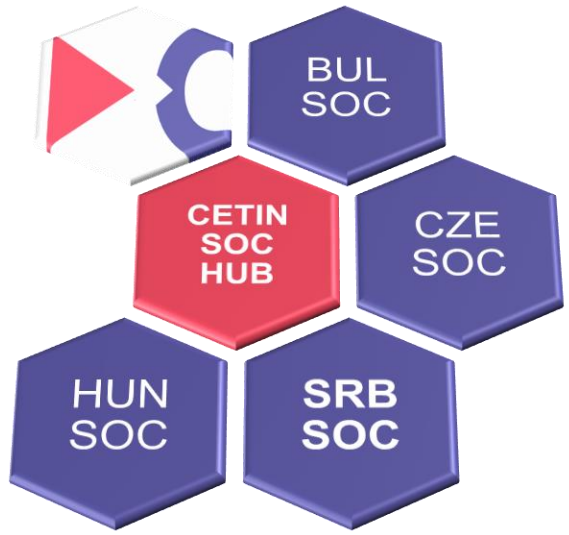
Detaljno upravljanje incidentima
Izbegavanje / Preporuke i izmene sistema

Nivo 3

Prediktivna analitika i analiza pretnji
Forenzika

Nivo 3+

Integracija i kolaboracija sa trećim stranama
Threat hunting
Samostalni razvoj alata za detekciju i sprečavanje pretnji

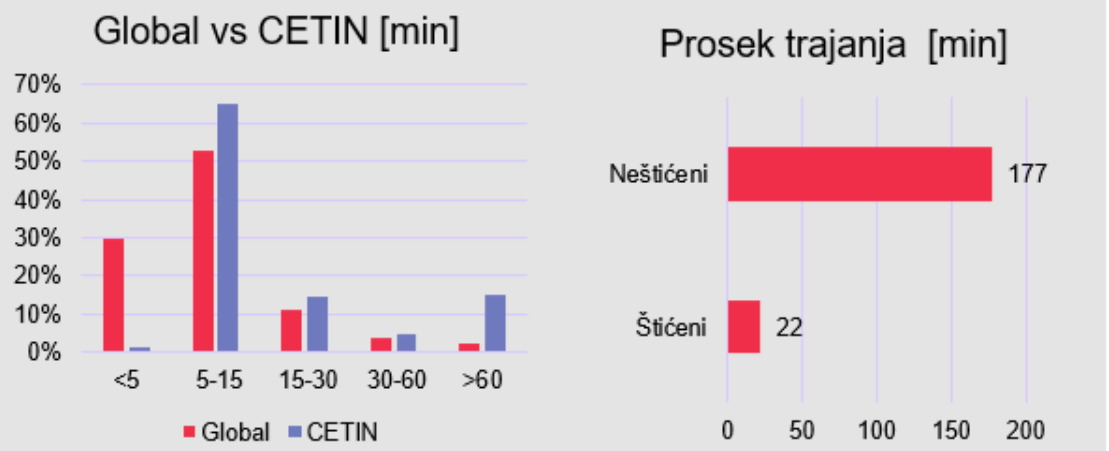


CETIN
MEMBER OF PPF GROUP

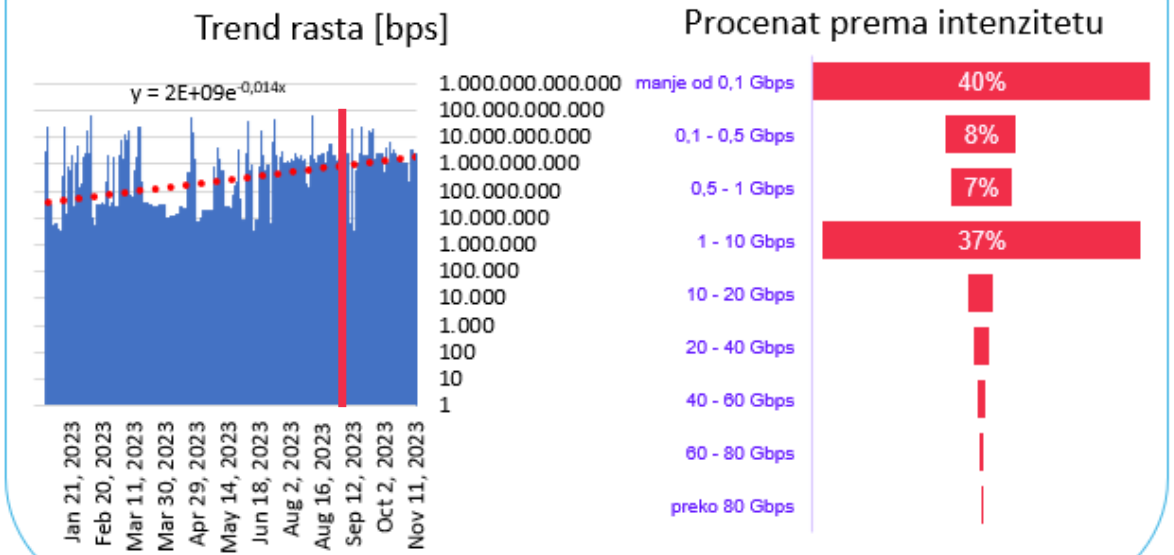
DDoS napadi na nezaštićene objekte traju 8x duže

Intenzitet napada prati trend rasta broja napada

Trajanje



Intenzitet



Najveći DDoS napad na CETIN infrastrukturu avgust 2023. - 101,3 Gbps

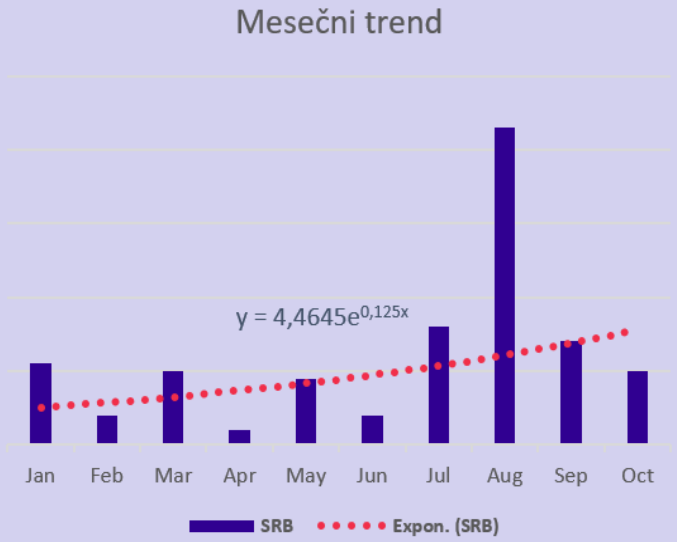
CETIN
MEMBER OF PPF GROUP

Izvor CETIN SOC

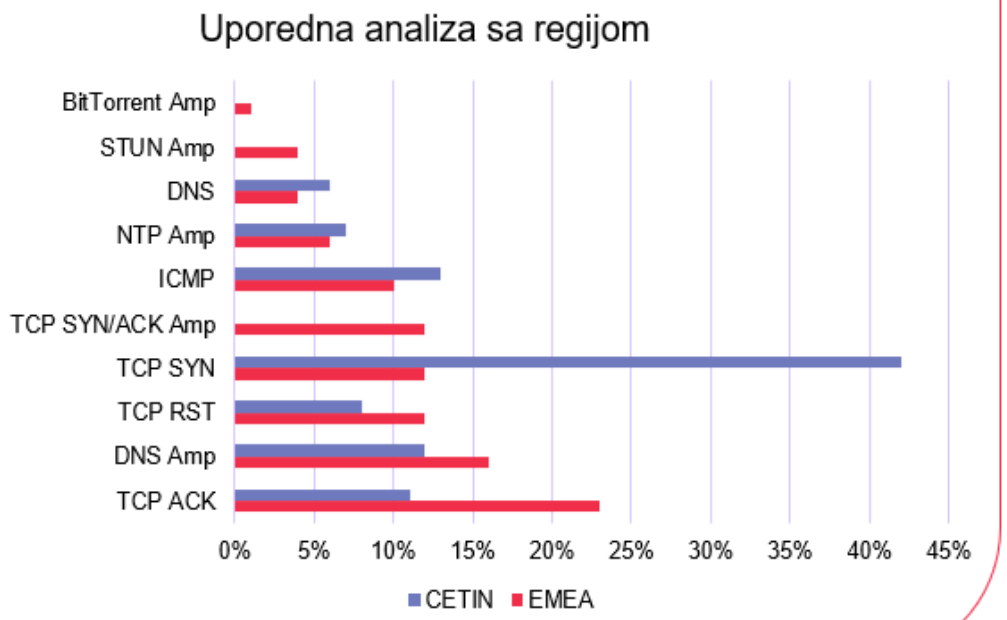
Učestalost broja napada raste

Tip napada je prilagođen objektu napada

Učestalost



Tipovi

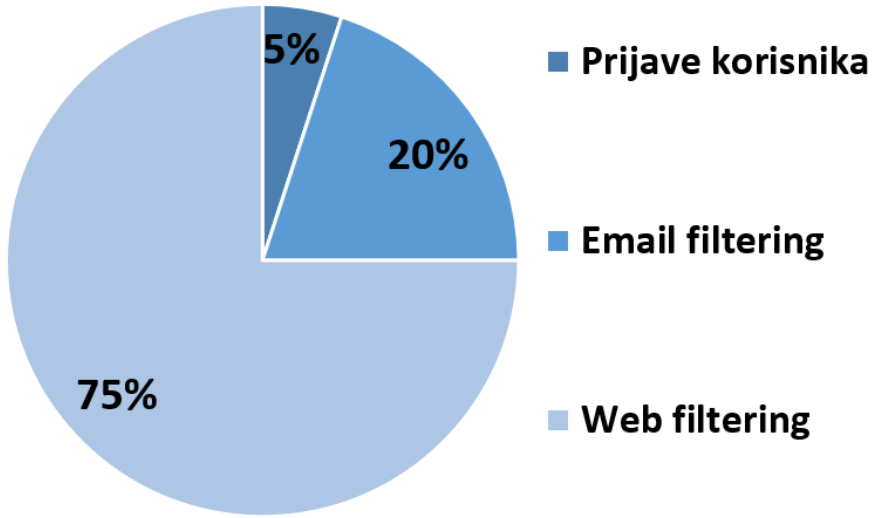


CETIN
MEMBER OF PPF GROUP

Izvor CETIN SOC

Više nivoa zaštite – manja ranjivost na Phishing

- Više Phishing vektora
  - Email
  - Web
  - Ostalo
- Tri osnovne metode zaštite
- 2023. godina, 7 kompanija, 4 države, preko 10.000 korisnika

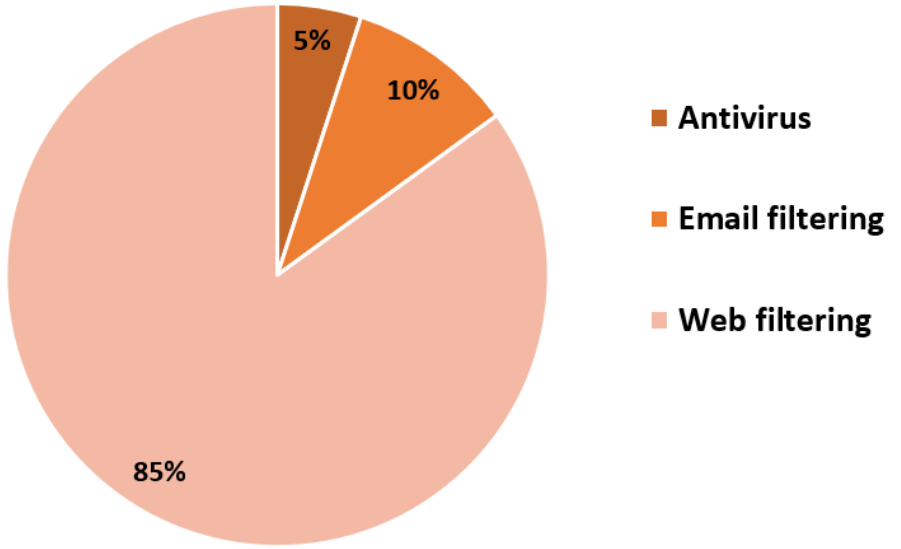


Sama obuka ne znači sigurnost.

Izvor: CETIN SOC

Višeslojna zaštita od Malware-a je efikasnija

- Više nivoa zaštite
- Uzorak sa 3 alata
- 2023. godina, 7 kompanija, 4 države, preko 10.000 korisnika



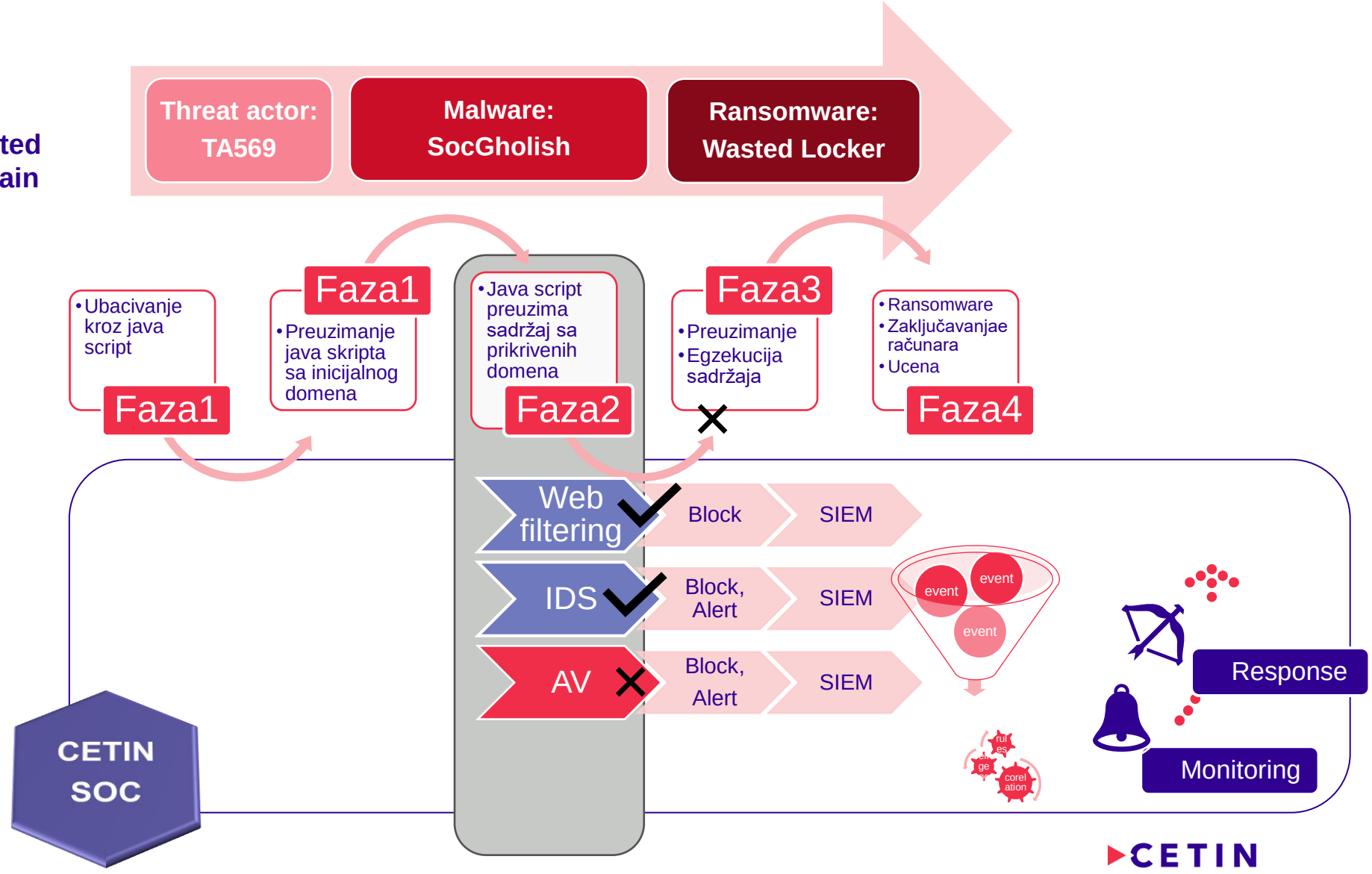
Antivirus nije dovoljan.

Izvor: CETIN SOC

Primer maliciozne aktivnosti u praksi

- 07.09.2023. IDS uočava malicioznu aktivnost
  - Exploit Kit Activity Detected [TA569 Keitaro TDS Domain in DNS Lookup
- Web filtering – blokirao dns zahteve:
  - backendjs.org
  - draggedline.org
  - ghost.blueecho88.com
  - linedgreen.org
  - throatpills.org
- Više AV skeniranja:
  - bez indikacija
- Analiza URL ukazuje na prvi korak ka pokušaju ubacivanja Ransomware-a.

2 od 3 raspoloživa alata su detektovala malver.



Šta smo zaključili?

- Integracija alata i kolaboracija u SOC – bolja detekcija napada
- Intenzitet napada prati trend rasta broja napada
- DDoS napadi na nezaštićene objekte traju 8x duže
- Napadi su prilagođeni žrtvi
- Više nivoa zaštite – manja ranjivost
- Sama obuka ne znači sigurnost
- Antivirus nije dovoljan

Hvala na pažnji!

info@cetin.rs

CETIN
MEMBER OF PPF GROUP