CUC2016

CARNetova korisnička konferencija

sys.trek

Javno dostupni servisi - početak jednog divnog DRDoS napada

Marko Stanec - CARNet

Projekt je sufinancirala Europska unija iz europskih strukturnih i investicijskih fondova. Više informacija o EU fondovima možete naći na web stranicama Ministarstva regionalnoga razvoja i fondova Europske unije: www.strukturnifondovi.hr

CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Europska unija
Zajedno do fondova EU

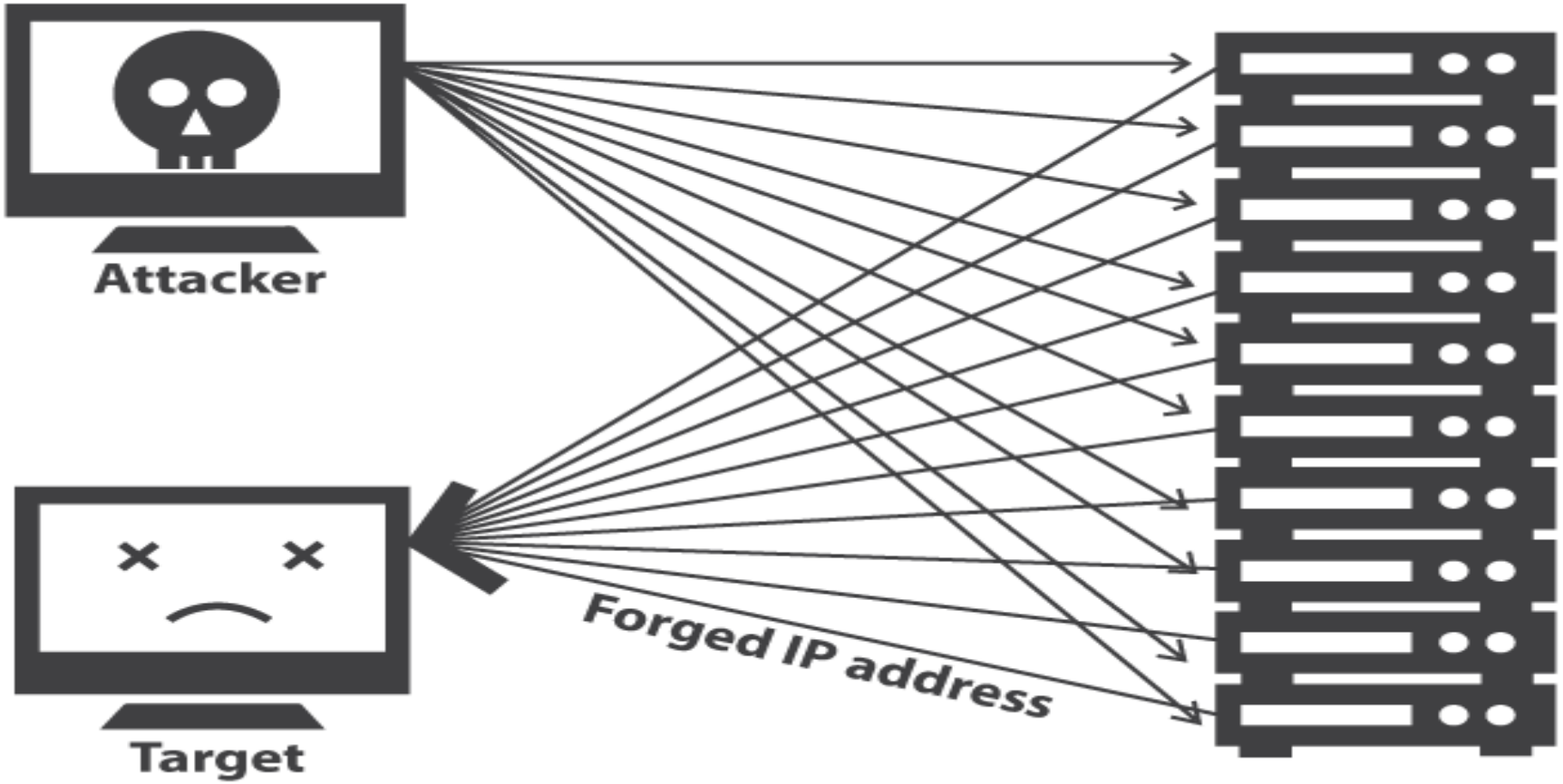
EUROPSKI STRUKTURNI I INVESTICIJSKI FONDOVI

ESF UČINKOVITI LJUDSKI POTENCIJALI

Operativni program KONKURENTNOST I KOHEZIJA

1TBPS DDOS ATTACK

THE BIGGEST ATTACK THIS WORLD HAS EVER SEEN


Attacker
Target
Forged IP address

shadowserver

- volonterska, neprofitna, vendor-free organizacija
- MISIJA:
  - poboljšati razinu sigurnosti na Internetu
- KAKO?
  - podizanjem svijesti o detektiranim botnet aktivnostima, kompromitiranim poslužiteljima te širenju malicioznog softvera slanjem izvještaja


Look at the bright side...
At least Mondays
only happen
once a week!

Izvještaji za javno dostupne servise

- DNS_openresolver
- MS-SQL
- NTP
- Portmapper
- SNMP
- SSDP

sys.portal CARNet

Arhiva seminara | CARNet web | sys.help | CARNet paketi | Kontakti

Kako ograničiti ili onemogućiti rpcbind?

Ukoliko ste ovih dana dobili poruku od CARNetove Abuse službe kako imate otvoren servis "portmapper", koji je predstavlja sigurnosni rizik, evo načina kako taj problem minimizirati, odnosno u potpunosti ga riješiti. Poruka koju smo dobili glasi otprilike ovako:

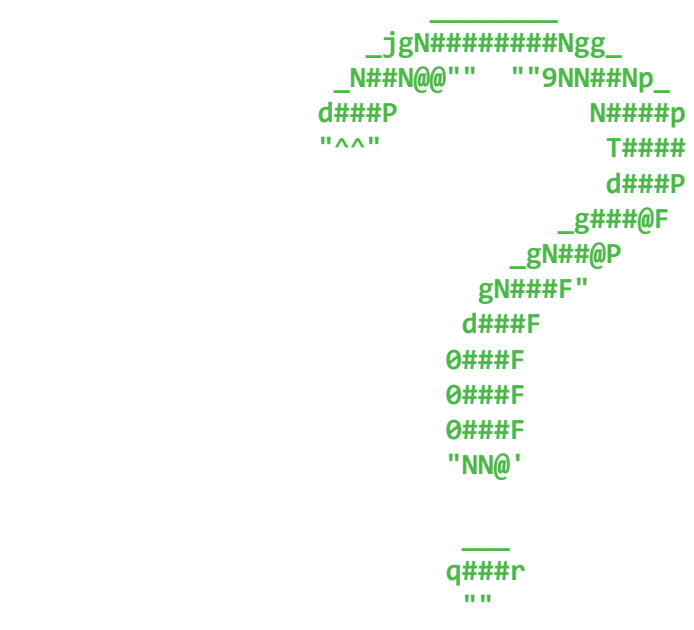
```
Postovani,

prilog sadrzi podatke o racunalima s aktivnim i javno dostupnim
Portmapper servisom.  Iako samo racunalo nije ranjivo pokrenuti
servis potencijalno moze biti iskoristen u DrDoS "amplification"
napadima. Dodatno moze biti iskoristen za pribavljanje velike
kolicine informacija o ciljanom uredjaju ako je dostupan program
"mountd".
```

„You can't defend. You can't prevent. The only thing you can do is detect and respond.”

Bruce Schneier

Hvala na pažnji!



CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Europska unija
Zajedno do fondova EU

EUROPSKI STRUKTURNI I INVESTICIJSKI FONDOVI

ESF UČINKOVITI LJUDSKI POTENCIJALI

Operativni program KONKURENTNOST I KOHEZIJA

Projekt je sufinancirala Europska unija iz europskih strukturnih i investicijskih fondova. Više informacija o EU fondovima možete naći na web stranicama Ministarstva regionalnoga razvoja i fondova Europske unije: www.strukturnifondovi.hr