ZAŠTITITE SVOJU FIRMU I ZAPOSLENE

# KAKO POSTUPITI UKOLIKO SE REALIZUJE DDoS NAPAD

PRIJAVITE SVAKI INCIDENT
NA NAŠEM PORTALU

SRB-CERT

# PRIPREMA

**Cilj: Uspostaviti kontakte, definisati procedure i prikupiti informacije kako biste uštedeli vreme tokom napada.**

## PODRŠKA INTERNET SERVIS PROVAJDERA (ISP)

- Obratite se pružaocu ISP usluga kako biste saznali koje usluge za ublažavanje DDoS napada imaju u svojoj ponudi (besplatne ili plaćene) i koji postupak treba da sledite. Pružaoci ISP usluga mogu da pomognu u preduzimanju radnji prilikom DDoS napada, u pogledu brzine i efikasnosti.
- Ako postoji mogućnost, pretplatite se na redudantnu Internet konekciju.
- Ako postoji mogućnost, pretplatite se na uslugu prevencije od DDoS napada kod vašeg provajdera.
- Ako postoji mogućnost, zatražite od ISP-a da postave filtere za portove i veličinu paketa.
- Uspostavite kontakte sa pružaocem internet usluga i organima za sprovođenje zakona. Proverite da li imate mogućnost korišćenja van opsega (*out-of-band*) kanala za komunikaciju (npr. telefon).
- Konfigurišite pravila na *firewall*-u kako bi se blokirao dolazni saobraćaj sa adresa izlistanih u RFC 5735, kao i rezervisanih IP adresa (0/8), loopback adresa (127/8), privatnih adresa (RFC 1918 blokirati 10/8, 172.16/12 i 192.168/16), unassigned DHCP client adresa (169.254.0/16) i multicast adresa (224.0.0/4). Ova podešavanja možete tražiti i od vašeg ISP-a.

## POPISNA LISTA

- Kreirajte listu tzv. *whitelist* IP adresa i protokola koje morate da propustite i na taj način odredite prioritete u saobraćaju tokom napada. Ne zaboravite da uključite vaše ključne stejkholdere u poslovanju.
- Dokumentujte detalje o vašoj IT infrastrukturi, uključujući nosioce posla, IP adrese i krug ID-jeva, podešavanja rutiranja (AS itd.); Pripremite dijagram topologije mreže i popis imovine.

## MREŽNA INFRASTRUKTURA

- Dizajnirajte mrežnu infrastrukturu tako da nemate jedinstvenu tačku otkaza (*Single Point of Failure*) ili usko grlo.
- Distribuirajte svoje DNS servere i druge kritične servise (SMTP, itd.) kroz različite AS.
- Ojačajte (*hardening*) konfiguraciju mreže, operativnih sistema i komponente aplikacija koje mogu biti cilj DDoS napada.

- Označite performanse vaše trenutne infrastrukture, tako da napad identifikujte brže i tačnije.
- Ako vaš posao zavisi od interneta, razmislite o kupovini specijalizovanih proizvoda ili usluga za ublažavanje posledica od DDoS napada. Ovu uslugu možete zatražiti i od vašeg ISP-a.
- Proverite podešavanja DNS *time-to-live* (TTL) za sisteme koji mogu biti napadnuti. Smanjite vrednost TTL-a ako je potrebno da biste olakšali DNS-u preusmeravanje u slučaju napada na originalne IP adrese. Preporučljivo podešavanje TTL-a je na 600s.
- U zavisnosti od kritičnosti vaših usluga, razmislite o podešavanju rezervne kopije koju možete uključiti u slučaju problema.
- Kako bi ojačali zaštitu od DDoS napada, povećajte propusni opseg na veb serveru. Ovim ne rešavate problem, već dobijate na vremenu da reagujete.
- Podesite niže pragove za SYN, ICMP i UDP pakete na mrežnim uređajima kako bi umanjili štetu od napada.

### INTERNI KONTAKTI

- Uspostavite kontakte između svojh timova za IDS, *firewall*, sistemsku i mrežnu podršku.
- Saradnja u okviru svih poslovnih linija da biste razumeli posledice koje ostavlja na poslovanje (npr. gubitak novca) mogući scenario DDoS napada.
- Uključite timove za BCP/DR (*Business Continuity Planning/Disaster Recovery*) u proces planiranja. Ovi planovi vam mogu pomoći u reagovanju prilikom DDoS napada.

**Fazu „pripreme“ treba smatrati najvažnijim elementom za uspešno reagovanje na DDoS incident.**

# IDENTIFIKACIJA

**Cilj: Otkriti incident, utvrditi njegov obim i odgovarajuće strane koje su uključene.**

Simptomi DDoS napada u nekim slučajevima mogu upućivati na nemaliciozne probleme, kao što su tehnički problemi na određenom delu mreže ili problemi nastali tokom održavanja od strane sistem administratora. Međutim, na sledeće simptome obratite pažnju jer mogu ukazivati na DoS ili DDoS napade:

- Usporene mrežne performanse (tokom otvaranja fajlova ili pristupa veb stranicama).
- Nedostupan veb sajt ili deo veb sajta.
- Nemogućnost pristupa bilo kom veb sajtu.

Najbolji način da se detektujete i identifikujete DDoS napad je kroz analizu i praćenje mrežnog saobraćaja, što možete postići preko *firewall-a* ili sistema za detekciju napada. Administratori mogu postaviti pravila za detekciju sumnjivog saobraćaja i identifikaciju izvora tog saobraćaja.

## ANALIZA NAPADA

- Potrebno je da razumete logički tok DDoS napada i identifikujte infrastrukturne komponente na koje je uticao, odnosno utvrditi lokacije gde je DDoS napad izvršen, analizom *firewall-a* za propuštene i odbijene pakete.
- Dostavite ISP-u IP adresu napadača.
- Potrebno je da uvidite da li ste meta napada ili kolateralna žrtva.
- Pogledajte opterećenje i logove fajlova sa servera, rutera, *firewall*-ova, aplikacija i druge pogođene infrastrukture. Kako bi smanjili štetu nastalu SYN Flood napadima. U podešavanjima na perifernim uređajima kao što su firewall i proxy serveri, podesite „*TCP keepalive*“ i „*Maximum Connections*“.
- Identifikujte sve aspekate koje DDoS saobraćaj razlikuju od normalnog saobraćaja, kao što su:
  → Izvornišne IP adrese, AS itd.
  → Odredišni portovi
  → URL adrese
  → Flag-ovi protokola
- Za analizu mreže mogu se koristiti alati za praćenje saobraćaja, kao što su: **Tcpdump, Tshark,WireShark, Snort, Argus, Ntop, Aguri, MRTG.**
- Ako je moguće, kreirajte NIDS (*Network Intrusion Detection Systems*) potpis da biste razlikovali normalni od zlonamernog saobraćaja.

## UKLJUČITE INTERNE I EKSTERNE AKTERE

- Obratite se svojim internim timovima da biste saznali kako oni vide napad.
- Tražite pomoć od svog ISP-a. Budite konkretni u vezi sa saobraćajem koji želite da kontrolišete:
  → Uključene mrežne blokove
  → Izvorišne IP adrese
  → Protokole
- Obavestite izvršne i pravne timove u okviru vaše kompanije.

## PROVERITE POZADINU

- Saznajte da li je kompanija dobila ponudu iznude pre samog napada.
- Proverite da li bi neko imao interes da preti vašoj kompaniji:
  → Konkurenti
  → Ideološki motivisane grupe (*hacktivists*)
  → Bivši zaposleni

# SPREČAVANJE DALJEG ŠIRENJA

**Cilj: Ublažiti efekte napada na ciljano okruženje.**

- Ako je usko grlo određena funkcija (*feature*) aplikacije, privremeno onemogućite tu funkciju.
- Pokušajte da regulišite ili blokirate DDoS saobraćaj ako je moguće što je bliže mrežnom „oblaku" preko rutera, *firewall*-a, *load balancer*-a, specijalizovanih uređaj i slično.
- Prekinuti neželjene veze ili procese ka serverima i ruterima i podesite njihova TCP/IP podešavanja.
- Ako je moguće, prebacite se na alternativne sajtove ili mreže koristeći DNS ili neki drugi mehanizam. *Blackhole* rutiranje DDoS saobraćaja koje je usmereno na originalne IP adrese.
- Postavite alternativni kanal za komunikaciju između vas i vaših korisnika/kupaca (npr: veb server, mejl server, voice server itd.)
- Ako je moguće, usmerite saobraćaj kroz servis ili uređaj za filtriranje saobraćaja (*traffic-scrubbing*) preko DNS -a ili promene rutiranja (npr: *sinkhole* rutiranje).
- Konfigurišite izlazne filtere tako da blokiraju saobraćaj u vašim sistemima i spreče slanje odgovora na DDoS saobraćaj (npr: *backsquatter* saobraćaj), da biste izbegli dodavanje suvišnih paketa u mreži.
- U slučaju pokušaja iznude od strane zlonamernog napadača, pokušajte da kupite vreme. Na primer, objasnite da vam treba više vremena kako biste dobili odobrenje rukovodstva.

**Ako je usko grlo na strani ISP-a, samo ISP može da preduzme efikasne akcije u vezi sprečavanja neželjenog saobraćaja. U tom slučaju, da biste rešili problem uskog grla potrebno je da radite zajednosa vašim ISP-om i obavezno podelite sve bitne informacije brzo i efikasno kako biste rešili problem u što kraćem roku.**

# SANACIJA

**Cilj: Preduzeti akcije za zaustavljanje DDoS napada**

- Obratite se ISP-u i uverite se da primenjuje mere za sanaciju. Neke od mogućih mera koje se mogu preduzeti:
  → Filtriranje (ako je moguće na nivou Tier 1 ili Tier 2)
  → Filtriranje saobraćaja (*Traffic-scrubbing*)/*Sinkhole*/*Clean-pipe)*
  → *Blackhole* rutiranje
- Ako su identifikovani DDoS napadači, razmotrite uključivanje tima za sprovođenje zakona. Izvršni i pravni tim rade dalje po procedurama vaše kompanije i zakona.

**Vaš ISP uglavnom pruža podršku za sanaciju tehničkih radnji.**

# OPORAVAK

**Cilj: Vratiti u prethodno funkcionalno stanje.**

## PROCENITE KRAJ DDoS NAPADA

- Proverite da li su usluge koje su bile pod uticajem napada ponovo dostupne.
- Proverite da li su sve performanse vaše infrastrukture vraćene na početno stanje.

## VRATITE SISTEM NA NORMALNO FUNKCIONISANJE

- Vratite saobraćaj na originalnu mrežu.
- Restartujte stopirane servise.

**Važno je da su akcije povezane sa oporavkom sistema usklađene sa mrežnim timovima. Vraćanje usluga može imati neočekivane posledice.**

# POSLEDICE

**Cilj: Dokumentujte detalje incidenta, diskutujte o naučenim lekcijama i prilagodite planove i odbranu.**

- Razmislite koje korake biste preduzeli kako bi brže ili efikasnije odgovorili na incident.
- Ako je potrebno, prilagodite pretpostavke koje su uticale na odluke donete tokom DDoS incidenta.
- Procenite efikasnost reagovanja na DDoS proces, koji uključuje ljude i komunikaciju.
- Razmislite o odnosima unutar i van vaše organizacije koje bi vam mogle pomoći u budućnosti u slučaju incidenta.
- Saradnja sa pravnim timom može imati veliki značaj, naročito ako je postupak u toku.

**Izvor:**

https://github.com/certsocietegenerale

Security Tip - Understanding Denial-of-Service Attacks - CISA

Guidance on Responding to Denial of Service Attack for SME - KISA

REPUBLIKA SRBIJA
RATEL
REGULATORNA AGENCIJA ZA ELEKTRONSKE KOMUNIKACIJE I POŠTANSKE USLUGE

#odbraniseznanjem

SRB-CERT