ЗАШТИТИТЕ СВОЈУ ФИРМУ И ЗАПОСЛЕНЕ

КАКО ПОСТУПИТИ УКОЛИКО СЕ РЕАЛИЗУЈЕ DDoS НАПАД

ПРИЈАВИТЕ СВАКИ ИНЦИДЕНТ
НА НАШЕМ ПОРТАЛУ

СРБ-ЦЕРТ

ПРИПРЕМА

Циљ: Успоставити контакте, дефинисати процедуре и прикупити информације како бисте уштедели време током напада.

ПОДРШКА ИНТЕРНЕТ СЕРВИС ПРОВАЈДЕРА (ИСП)

- Обратите се пружаоцу ИСП услуга како бисте сазнали које услуге за ублажавање DDoS напада имају у својој понуди (бесплатне или плаћене) и који поступак треба да следите. Пружаоци ИСП услуга могу да помогну у предузимању радњи приликом DDoS напада, у погледу брзине и ефикасности.
- Ако постоји могућност, претплатите се на редудантну Интернет конекцију.
- Ако постоји могућност, претплатите се на услугу превенције од DDoS напада код вашег провајдера.
- Ако постоји могућност, затражите од ИСП-а да поставе филтере за портове и величину пакета.
- Успоставите контакте са пружаоцем интернет услуга и органима за спровођење закона. Проверите да ли имате могућност коришћења ван опсега (*out-of-band*) канала за комуникацију (нпр. телефон).
- Конфигуришите правила на *firewall*-у како би се блокирао долазни саобраћај са адреса излистаних у RFC 5735, као и резервисаних IP адреса (0/8), loopback адреса (127/8), приватних адреса (RFC 1918 блокирати 10/8, 172.16/12 и 192.168/16), unassigned DHCP client адреса (169.254.0/16) и multicast адреса (224.0.0/4). Ова подешавања можете тражити и од вашег ИСП-а.

ПОПИСНА ЛИСТА

- Креирајте листу тзв. *whitelist* IP адреса и протокола које морате да пропустите и на тај начин одредите приоритете у саобраћају током напада. Не заборавите да укључите ваше кључне стејкхолдере у пословању.
- Документујте детаље о вашој ИТ инфраструктури, укључујући носиоце посла, IP адресе и круг ИД-јева, подешавања рутирања (AS итд.); Припремите дијаграм топологије мреже и попис имовине.

МРЕЖНА ИНФРАСТРУКТУРА

- Дизајнирајте мрежну инфраструктуру тако да немате јединствену тачку отказа (*Single Point of Failure*) или уско грло.
- Дистрибуирајте своје DNS сервере и друге критичне сервисе (SMTP, итд.) кроз различите AS.
- Ојачајте (*hardening*) конфигурацију мреже, оперативних система и компоненте апликација које могу бити циљ DDoS напада.

- Означите перформансе ваше тренутне инфраструктуре, тако да напад идентификујте брже и тачније.
- Ако ваш посао зависи од интернета, размислите о куповини специјализованих производа или услуга за ублажавање последица од DDoS напада. Ову услугу можете затражити и од вашег ИСП-а.
- Проверите подешавања DNS *time-to-live* (TTL) за системе који могу бити нападнути. Смањите вредност TTL-а ако је потребно да бисте олакшали DNS-у преусмеравање у случају напада на оригиналне IP адресе. Препоручљиво подешавање TTL-а је на 600s.
- У зависности од критичности ваших услуга, размислите о подешавању резервне копије коју можете укључити у случају проблема.
- Како би ојачали заштиту од DDoS напада, повећајте пропусни опсег на веб серверу. Овим не решавате проблем, већ добијате на времену да реагујете.
- Подесите ниже прагове за SYN, ICMP и UDP пакете на мрежним уређајима како би умањили штету од напада.

ИНТЕРНИ КОНТАКТИ

- Успоставите контакте између својх тимова за IDS, *firewall*, системску и мрежну подршку.
- Сарадња у оквиру свих пословних линија да бисте разумели последице које оставља на пословање (нпр. губитак новца) могући сценарио DDoS напада.
- Укључите тимове за BCP/DR (*Business Continuity Planning*/*Disaster Recovery*) у процес планирања. Ови планови вам могу помоћи у реаговању приликом DDoS напада.

Фазу „припреме“ треба сматрати најважнијим елементом за успешно реаговање на DDoS инцидент.

ИДЕНТИФИКАЦИЈА

Циљ: Открити инцидент, утврдити његов обим и одговарајуће стране које су укључене.

Симптоми DDoS напада у неким случајевима могу упућивати на немалициозне проблеме, као што су технички проблеми на одређеном делу мреже или проблеми настали током одржавања од стране систем администратора. Међутим, на следеће симптоме обратите пажњу јер могу указивати на DoS или DDoS нападе:

- Успорене мрежне перформансе (током отварања фајлова или приступа веб страницама).
- Недоступан веб сајт или део веб сајта.
- Немогућност приступа било ком веб сајту.

Најбољи начин да се детектујете и идентификујете DDoS напад је кроз анализу и праћење мрежног саобраћаја, што можете постићи преко *firewall*-а или система за детекцију напада. Администратори могу поставити правила за детекцију сумњивог саобраћаја и идентификацију извора тог саобраћаја.

АНАЛИЗА НАПАДА

- Потребно је да разумете логички ток DDoS напада и идентификујте инфраструктурне компоненте на које је утицао, односно утврдити локације где је DDoS напад извршен, анализом *firewall*-а за пропуштене и одбијене пакете.
- Доставите ИСП-у IP адресу нападача.
- Потребно је да увидите да ли сте мета напада или колатерална жртва.
- Погледајте оптерећење и логове фајлова са сервера, рутера, *firewall*-ова, апликација и друге погођене инфраструктуре. Како би смањили штету насталу SYN Flood нападима. У подешавањима на периферним уређајима као што су *firewall* и *proxy* сервери, подесите „*TCP keepalive*“ и „*Maximum Connections*“.
- Идентификујте све аспекате које DDoS саобраћај разликују од нормалног саобраћаја, као што су:
  → Изворнишне IP адресе, AS итд.
  → Одредишни портови
  → URL адресе
  → Flag-ови протокола
- За анализу мреже могу се користити алати за праћење саобраћаја, као што су: **Tcpdump, Tshark, WireShark, Snort, Argus, Ntop, Aguri, MRTG.**
- Ако је могуће, креирајте NIDS (*Network Intrusion Detection Systems*) потпис да бисте разликовали нормални од злонамерног саобраћаја.

УКЉУЧИТЕ ИНТЕРНЕ И ЕКСТЕРНЕ АКТЕРЕ

- Обратите се својим интерним тимовима да бисте сазнали како они виде напад.
- Тражите помоћ од свог ИСП-а. Будите конкретни у вези са саобраћајем који желите да контролишете:
  → Укључене мрежне блокове
  → Изворишне IP адресе
  → Протоколе
- Обавестите извршне и правне тимове у оквиру ваше компаније.

ПРОВЕРИТЕ ПОЗАДИНУ

- Сазнајте да ли је компанија добила понуду изнуде пре самог напада.
- Проверите да ли би неко имао интерес да прети вашој компанији:
  → Конкуренти
  → Идеолошки мотивисане групе (*hacktivists*)
  → Бивши запослени

СПРЕЧАВАЊЕ ДАЉЕГ ШИРЕЊА

Циљ: Ублажити ефекте напада на циљано окружење.

- Ако је уско грло одређена функција (*feature*) апликације, привремено онемогућите ту функцију.
- Покушајте да регулишите или блокирате DDoS саобраћај ако је могуће што је ближе мрежном „облаку“ преко рутера, *firewall*-а, *load balancer*-а, специјализованих уређај и слично.
- Прекинути нежељене везе или процесе ка серверима и рутерима и подесите њихова TCP/IP подешавања.
- Ако је могуће, пребаците се на алтернативне сајтове или мреже користећи DNS или неки други механизам. *Blackhole* рутирање DDoS саобраћаја које је усмерено на оригиналне IP адресе.
- Поставите алтернативни канал за комуникацију између вас и ваших корисника/купаца (нпр: веб сервер, мејл сервер, voice сервер итд.)
- Ако је могуће, усмерите саобраћај кроз сервис или уређај за филтрирање саобраћаја (*traffic-scrubbing*) преко DNS -а или промене рутирања (нпр: *sinkhole* рутирање).
- Конфигуришите излазне филтере тако да блокирају саобраћај у вашим системима и спрече слање одговора на DDoS саобраћај (нпр: *backsquatter* саобраћај), да бисте избегли додавање сувишних пакета у мрежи.
- У случају покушаја изнуде од стране злонамерног нападача, покушајте да купите време. На пример, објасните да вам треба више времена како бисте добили одобрење руководства.

Ако је уско грло на страни ИСП-а, само ИСП може да предузме ефикасне акције у вези спречавања нежељеног саобраћаја. У том случају, да бисте решили проблем уског грла потребно је да радите заједно са вашим ИСП-ом и обавезно поделите све битне информације брзо и ефикасно како бисте решили проблем у што краћем року.

САНАЦИЈА

Циљ: Предузети акције за заустављање DDoS напада

- Обратите се ИСП-у и уверите се да примењује мере за санацију. Неке од могућих мера које се могу предузети:
  → Филтрирање (ако је могуће на нивоу *Tier* 1 или *Tier* 2)
  → Филтрирање саобраћаја (*Traffic-scrubbing*)/*Sinkhole*/*Clean-pipe)*
  → Blackhole рутирање
- Ако су идентификовани DDoS нападачи, размотрите укључивање тима за спровођење закона. Извршни и правни тим раде даље по процедурама ваше компаније и закона.

Ваш ИСП углавном пружа подршку за санацију техничких радњи.

ОПОРАВАК

Циљ: Вратити у претходно функционално стање.

ПРОЦЕНИТЕ КРАЈ DDoS НАПАДА

- Проверите да ли су услуге које су биле под утицајем напада поново доступне.
- Проверите да ли су све перформансе ваше инфраструктуре враћене на почетно стање.

ВРАТИТЕ СИСТЕМ НА НОРМАЛНО ФУНКЦИОНИСАЊЕ

- Вратите саобраћај на оригиналну мрежу.
- Рестартујте стопиране сервисе.

Важно је да су акције повезане са опоравком система усклађене са мрежним тимовима. Враћање услуга може имати неочекиване последице.

ПОСЛЕДИЦЕ

Циљ: Документујте детаље инцидента, дискутујте о наученим лекцијама и прилагодите планове и одбрану.

- Размислите које кораке бисте предузели како би брже или ефикасније одговорили на инцидент.
- Ако је потребно, прилагодите претпоставке које су утицале на одлуке донете током DDoS инцидента.
- Проценитe ефикасност реаговања на DDoS процес, који укључује људе и комуникацију.
- Размислите о односима унутар и ван ваше организације које би вам могле помоћи у будућности у случају инцидента.
- Сарадња са правним тимом може имати велики значај, нарочито ако је поступак у току.

Извор:

https://github.com/certsocietegenerale

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

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