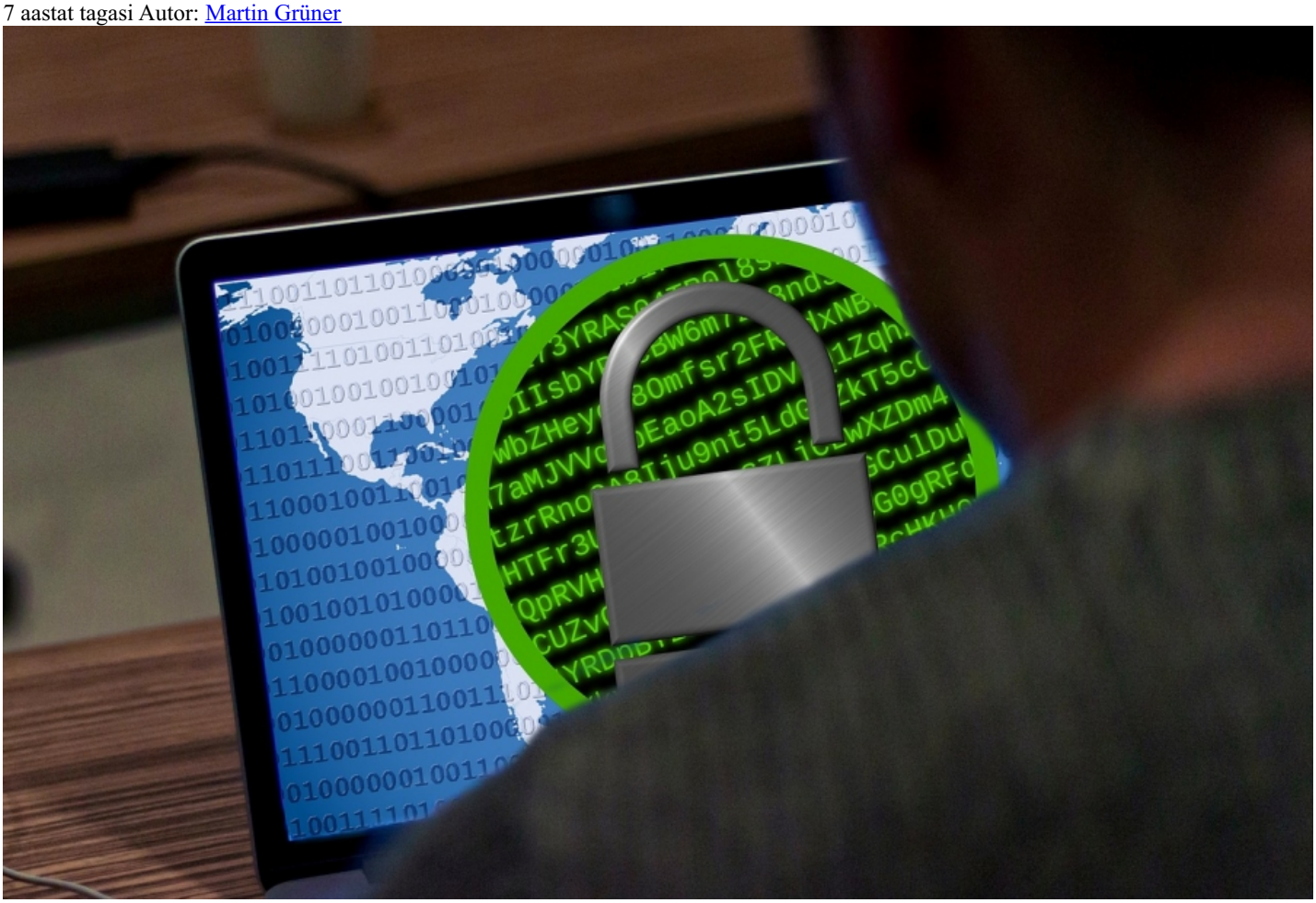
Mis on DDoS rünnak ja kuidas end selle eest kaitsta?

7 aastat tagasi Autor: Martin Grüner



Kui õngitsemine on levinuim eraisikute vastu suunatud rünnaku vorm internetis, siis DDoS on seda ettevõtete ja isegi riikide vastu. DDoS rünnaku eest pole kaitstud keegi ning seda on väga raske peatada, ennetada ja tõrjuda.

Mis on DDoS rünnak?

Täheühend ddos tuleb inglise inglise keelsetest sõnadest "*Distributed Denial of Service*", mida võib tõlkida, kui hajutatud teenuse tõkestamise rünnak. Tihti kasutatakse just seda tõlget, kuid minumeelest on see liialt pikk ja lohisev, mistõttu kasutan järgnevalt alati lihtsalt lühendit DDoS.

DDoS rünnak seisneb sihtmärgi päringutega nii ülekoormamises, et see muutub kättesaamatuks või kokku jookseb. Suure koormuse all võib iga veebileht või süsteem kättesaamatuks muutuda, tihti on seda juhtunud näiteks maksuametiga tuludeklaratsioonide esitamise alguses. Väga paljud soovivad olla esimeste seas, kes tagastuse saavad, mistõttu tahavad nad esitada deklaratsiooni võimalikult vara. Kuna maksuameti infosüsteem pole loodud sellise koormuse jaoks, võivad paljud näha lehe asemel veateadet.

DDoS rünnaku puhul tekitatakse süsteemile samuti koormus, kuid selle taga pole päris kasutajad. Kasutades mitmeid arvuteid saadab häkker sihtmärgi pihta suure koguse liiklust, mis selle tegevuse halvab.

> Kurjategija paneb ddos rünnaku toime kasutades pahavaraga naktunud arvuteid

Rünnaku läbiviimiseks ei kasuta häkker enamasti mitte omale kuuluvaid arvuteid, vaid arvutivõrke. Rünnaku paneb ta toime pahavaraga nakatunud arvutite kaudu, mille kasutajad ei ole enamasti ise teadlikud, et nende arvuti parasjagu kedagi päringutega pommitab. Sellist võrku nimetatakse botnetiks ning nakatunud arvuteid zombideks. Enamiku tänapäeva pahavara eesmärk ongi üle võtta arvuti ning kasutada seda rünnakuteks ning SPAM kirjade saatmiseks – ajad, kui viiruste eesmärk oli arvutit kahjustada, jäävad mineviku.

Mida rohkem on botnet'is nakatunud arvuteid, seda võimsama rünnaku kurjategija korraldada saab. Tegemist ei ole ammu noorte nohikute mässumeelse tegevuse vaid süsteemse ja koordineeritud äriga. Suurimad botnetid koosnevad miljonitest nakatunud arvutitest. "Mustas internetis" (Darknet) müüvad viiruste loojad rünnaku teenust aja (enamasti päev või nädal) kaupa.

> DDoS rünnakud on eriti ohtlikud, kuna neid on lihtne ja odav läbi viia

Häkkeri vaatepunktist pole midagi lihtsamat, kui saata kellegi suunas andmeid. See on täpselt see, mida su veebilehitseja tegi siia lehele tulles. Kuna ddos rünnaku läbi viimine ei vaja peaaegu mingeid oskusi ega turvaaukude ekspluateerimist, saab sellega hakkama iga interneti-pahalane.

Samuti on botnetide rentimine odav. Kuna erinevaid botnete on palju, ei ole rünnakute teenuse tellimine kallis. Kõigest 150 dollari eest võib tellida rünnaku mõne kodulehe/infosüsteemi pihta nädalaks. Tugevamad rünnakud on küll kallimad, kuid see annab aimu suurusjärgust. Ebaeetiline konkurent võib su kodulehe potensiaalselt nädalaks ligipääsmatuks muuta kõigest 20 dollariga päevas.

DDoS rünnak võib tulla igast seadmest

Kuna DDoS rünnakus osalemiseks ei pea seade olema võimeline tegema muud, kui saatma päringut, saab selleks kasutada palju lihtsamaid seadmeid, kui seda on arvutid. Nutitelefone nakatavad ussviirused on juba laialdaselt levinud, kuid ka palju lihtsamaid seadmeid saab rünnaku jaoks kasutada.

Oktoobris 2016 langes üks maailma juhtivaid internetiturvalisuse blogisid Kerbonsecurity massiivse DDoS rünnaku ohvriks, mis tuli haavatava tarkvaraga IP kaameratest. Ründaja oli oma botneti ehitanud uuendamata tarkvaraga IP kaameraid nakatades ning ründas blogi enam, kui 145 000 seadmest korraga. Nende omanikel polnud aimugi, et nende turvalisuse tagamiseks soetatud IP kaamerast oli vahepeal saanud zombi.

Potensiaalsed kaotused DDoS rünnaku ohvriks langemisel on piiritud

Ddos rünnaku ohvriks langedes ei pääse kliendid enam ligi su kodulehele, mistõttu saad sa vähem päringuid. Kui su äri on oma olemuselt internetis, näiteks e-poe kujul, jääb see täiesti seisma. Samuti paneb Google tähele, et su koduleht on maas, mis teeb suurt kahju su positsioonile otsingutulemustes ka peale rünnaku lõppu.

Miks on DDoS rünnakuid raske tõrjuda

DDoS rünnakute tõrjumine ja ennetamine on väga raske, kohati lausa võimatu. Seda sellepärast, et tihti on rünnak eristamatu päris liiklusest. Kui su süsteem on loodud 10 kasutaja jaoks, kuid järku kasutab seda 100 võib see kokku kukkuda. Samas pole tegemist rünnakuga, kõik 100 kasutajat on seal põhjusega. Kui ründaja suudab simuleerida neist sajast kasutajast 50t ei ole võimalik eristada millised päringud tulevad päris inimestelt ja millised zombidelt.

DDoS rünnaku tõrjumine on keeruline, kuna rünnak on hajutatud

Kui kogu rünnak tuleks ühest arvutist saaks selle IP lihtsalt blokeerida ja lahing oleks läbi. Kuna rünnakul on sadu, tuhandeid või potensiaalselt miljoneid alguspunkte, pole kuidagi võimalik kõigi nende ligipääsu blokeerida. Eriti arvestades, et nad pole enamasti (tõsi, see oleneb juba konkreetsest rünnaku tüübist) eristatavad legitiimsetest päringutest.

Näiteid DDoS rünnakutest

Ilmselt on kõigil meeles pronksiöö järgne küberrünnak Eesti riigiasutuste ja infosüsteemide vastu. See oli DDoS rünnak, mille eesmärk oli need ligipääsmatuks muuta.

Tegemist oli ühe ajaloo suurima DDoS rünnakuga riigistruktuuri pihta.

2014 jõulude ajal langesid DDoS rünnaku ohvriks nii Sony Playstation Network, kui Microsoftile kuuluv Xbox live. Rünnakul polnud muud motivatsiooni, kui mängureid ärritada ja ettevõtete äritegevust kahjustada. Ründajad on tänaseks tabatud, kellest üks oli kõigest 17-aastane Soome noormees. Ta mõisteti süüdi enam, kui 50 000 küberkuritegevuse juhus. Sama grupeering pani “lihtsalt nalja pärast” toime suurel hulgal erinevaid kuritegusid pommiähvardustest DDoS rünnakuteni.

Suure tõenäosusega suurim ddos rünnaks siiani toimus 2016 aasta esimestel tundidel BBC uudistevõrgu pihta. Ründajad saatsid nende vastu enam, kui 600 gigabaiti andmeid sekundis. Enamasti ei ületa DDoS rünnaku tugevus 40 gigabaiti sekundis.

Kuidas kaitsta oma ettevõtet DDoS rünnaku eest

Kuna ddos rünnakuid on erinevaid peab rakendama mitmeid kaitsemeetodeid. Täieliku kaitset ddos rünnaku vastu pakkuda võimalik pole, küll saad vähendada riski, et rünnak edukas on ning su kodulehe või teenuse kättesaamatuks muudab. Oluline on potensiaalseks rünnakuks alati valmis olla. Märgatavalt lihtsam on rünnakut ennetada, kui juba alanud rünnakut peatada.

Rakenduste pihta suunatud rünnakute eest kaitsevad regulaarsed tarkvarauuendused. Iga tarkvarauuendus tuleks installeerida esimesel võimalusel. Reeglina on turvapaigad iga tarkvaratootja jaoks prioriteetsed ning need väljastatakse esimesel võimalusel peale haavatavuse avastamist.

Füüsiline tulemüür aitab tõrjuda ddos rünnakut

Kui kogu infrasüsteem on sinu kontrolli all saad kasutada füüsilisi tulemüüre. Füüsiline tulemüür on seade, mis seisab sinu rakenduse serverite ning interneti vahel ning analüüsib ja filtreerib liiklust reaalajas. Füüsilised tulemüürid on efektiivsed, kuid kallid.

Soodsaim viis ddos rünnaku tõrjumiseks on pilvepõhine kaitseteenus

Pilvepõhise ddos kaitse teenuse pakkujaid on mitmeid, kuid soovitaks kasutada **KoDDOSi** teenust. Neil on erinevad paketid sõltuvalt su teenuse kriitilisusest. Nende valikust leiad veebimajutuse paketi, kus on juba olemas ddos rünnakute filter ning eraldi kaitseteenuse. Lisainfot leiad Koddosi koduleheelt siin.

Kaitseteenus on põhimõtteliselt VPN su serverile – kõik internetiliiklus läheb seda kasutades enne su veebilehe või teenuseni jõudmist läbi nende serveri. Koddosi serveripark on võimeline filtreerima pahatahtliku liiklust ning enam, kui 350 Gbps rünnaku ümber suunama.

Ddos rünnaku tüübid

Jätsin antud sektsiooni artikli lõppu, kuna see on eelnevast oluliselt tehnilisem. Oluline on teada, mis vormis võivad tulla ddos rünnakud, ning mida nad endast tehniliselt kujutavad. Paraku vajab see üksjagu teoreetilisi teadmisi võrguprotokollide tööst – annan allpool endast parima, et need võimalikult arusaadavalt lahti seletada.

Enamiku ddos rünnakuid jaotuvad rakenduse- ja mahupõhisteks rünnakuteks.

Rakendusepõhine rünnak kasutab ära haavatavust mõnes su serverisse installeeritud tarkvaras. Seda tüüpi ddos rünnaku korral saadab kurjategija su teenusele päringuid, mis on mõeldud antud rakendusele. Tihti on nii võimalik server täiesti kokku jooksutada. Rakendusepõhised rünnakud on haruldasemad, kui mahupõhised, kuna nõuavad ründajalt üksjagu eeltööd ning on reeglina suunatud just valitud sihtmärgi vastu.

Mahupõhised rünnakud seisnevad sihtmärgi suunas väga suure koguse liikluse saatmises. Nii on võimalik üle koormata ka kõige kiirema internetiühendusega ning võimsaima riistvaraga süsteemid. Mahupõhine rünnak võib tulla mitmes vormis. Järgnev on valik, absoluutselt mitte täielik nimekiri, erinevatest mahupõhistest ddos rünnaku tüüpidest.

UDP Flood – Enne, kui saame vaadata UDP flood rünnaku tööpõhimetet on paslik üle käia sellega seotud terminid.

UDP on internetipõhine andmeside protokoll, mida kasutavad paljud rakendused. Olles välja töötatud aastal 1980, on tegemist on ühe vanima ja levinuima võrguliikluse protokolliga.

Võrgu pakett (inglise keeles *network packet*) on üks väike osa päringust. Paljud protokollid, muuhulgas UDP, jaotavad suuremad päringud väikesteks osadeks, ehk pakettideks. UDP protokolli ei huvita pakettide sisu – tema ülesanne on need ainult kohale toimetada. Paketid paneb algseks päringuks kokku rakendus. Iga rakendus kuulab liiklust ühel pordil – nii saad korraga kasutada Skype ja mängida võrgumängu – kummagi liiklus toimub üle UDP, kuid erineval pordil.

UDP fllood (UDP “üleujutus” inglise keeles) rünnaku korral saadab häkker sihtmärgi pihta suurel kogusel UDP pakette täiesti suvalisel pordil, mida ei kasuta ükski rakendus. Iga uue paketiga peab sihtmärgi operatsioonisüsteem kontrollima rakendust, mis antud paketti kasutada oskaks. Suure hulga pakettide korral võtab see nii palju resursse, et teenus muutub kättesaamatuks.

TCP SYN Flood – Peale UDP on teine levinuim võrguliikluse protokoll TCP. TCP protokolli kasutatakse juhul, kui kõigi saadetud andmete kohalejõudmine on oluline. Näiteks tahad sa ilmselt, et sinuni jõuaks kogu e-kiri või allalaetud fail. Mõnel puhul pole see nii oluline – kui üks pakett Skype vestlusest või Netflixi videost peaks kaduma minema ei saa sa suure tõenäosusega sellest arugi. Sellisel juhul kasutatakse enamasti eelmises lõigus kirjeldatud UDP protokolli.

SYN flood rünnaku korral kasutab ära häkker ära TCP protokolli disaini sihtmärgi üle koormamiseks. Nimelt algab iga TCP ühendus “kolmekordse käepigistusega”. Toome lihtsustatud näitena, mis juhtub, kui kirjutad aadressiribale “netsec.ee”

1. Sinu veebilehitseja saadab päringu netsec.ee serverisse “tutvustades ennast”
2. Netsec.ee server vastab su veebilehitsejale teatega, et ta on päringu kätte saanud ning on valmis looma ühenduse
3. Su veebilehitseja vastab omakorda netsec.ee-le, et on ühenduse kätte saanud
4. Su veebilehtiseja ja Netsec.ee vahel on loodud ühendus, mis võimaldab andmeid (nagu see artikkel) edastada

SYN Flood rünnaku korral toimuvad esimesed 2 punkti zombistatud arvuti/seadme ja sihtmärgi vahel nagu peaks. Küll ei vasta zombi enam serveri päringule ning server jääb mõneks ajaks vastust ootama. Vastust ei tulegi, kuid häkker avab tänu zombistatud arvutite armeele väga suurel hulgal ühendusi serveriga, mis selle lõpuks “üle ujutavad” ning teenuse kättesaamatuks muudavad.

Ping of death – Ilmselt oled kuulnud terminit “ping”. Ping on programm, mis saadab serverile väikesemahulise päringu, millele see omakorda vastab. Seda kasutatakse enamasti kontrollimaks, kas teenus on kättesaadav ning kui kiirelt see päringule vastab. Ilmselt ei tule üllatusena, et seda saab ka kurjasti ära kasutada.

Andmekogus, mis saadetakse ühe pingiga on enamasti väike ja mahub ühte paketti (paketi definitsioon on “UDP Flood” rünnaku kirjelduse juures), kuid tegelikult võib sõnum olla suurem – kuni 65,535 baiti. Sellisel juhul jaotatakse see mitmeks paketiks. Kui saadetud pakettide maht on suurem, kui 65,535 võib see tekitada mälulekke, mis aja jooksul sihtmärgi kokku jooksutab.

Peegeldatud rünnakud – Peegeldatud (tihti kasutatakse ka terminit “võimendatud”) rünnakud on ohtlikud, kuna ründajal ei pea endal nende kasutuseks väga suurt botneti olema. Peegeldatud DDOS rünnakus korral saadab häkker päringuid kolmanda osapoole võrkudesse jättes mulje, et need tulevad rünnaku sihtmärgilt. Inglise keeles kasutatakse selleks terminit “IP aadress spoofing”, mida võib tõlkida, kui “IP aadressiga tüssamine”. IP aadressiga tüssamine on kahjuks lihtsam, kui arvata võib, mis muudab peegeldatud rünnakute läbiviimise üsna lihtsaks.

Peegeldaja saadab vastused päringule enam mitte ründajale või rünnakuks kasutatud zombile, vaid sihtmärgile. Õigete tehnikatega võib ründaja võrku saata ühe päringu, mis peegeldatakse sihtmärgini saja, võibolla isegi tuhande kordselt. Seetõttu on oluline oma ettevõtte arvutivõrgu ja serveripargi turvalisuses kontrollida, et sind ei saaks rünnaku peeglina/võimendina kasutada.

HTTP flood – HTTP flood seisneb sihtmärgi ülekoormamises HTTP päringutega. HTTP on protokoll, millel jooksevad kõik veebilehed. Kui vaatad aadressiribale, siis algavad kõik veebilehtede aadressid http:// või https://, millest viimane on lihtsalt krüpteeritud versioon HTTPst.

HTTP flood on suure tõenäosusega kõige ohtlikum rünnku tüüp, kuna seda on väga keeruline blokeerida. Rünnakuks kasutatakse täiesti legitiimseid päringuid, lihtsalt väga suurel hulgal. Tihti suunatakse päring su süsteemi komponendi pihta, mis kõige rohkem serveri

resursse võtab – tihti on selleks otsing. Ründajal pole probleem saata tuhandeid päringuid kõige keerulisema otsinguga su süsteemi pihta, mis kõik serveris resursinõudliku päringu käitavad. See võtab nii serveri, kui võrgu resursse ning muudab lõpuks teenuse kättesaamatuks.

MARTIN GRÜNER
Lugu ilmus Netsec.ee blogis

- Uudised
- Turvalisus