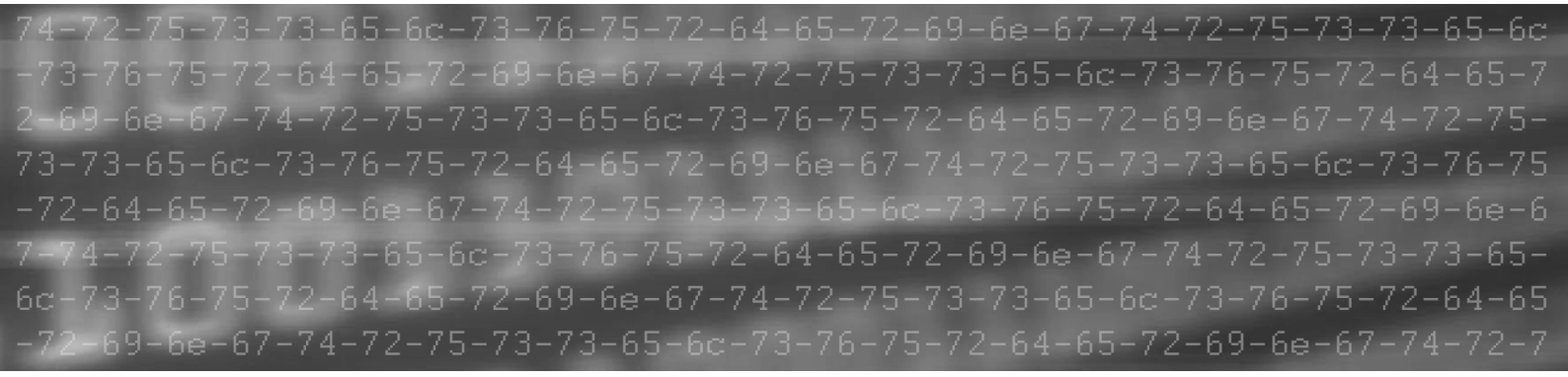
CENTER FOR
CYBERSIKKERHED

Trusselsvurdering

DDoS-angreb stiger i antal og størrelse



Trusselsvurderingsenheden ved Center for Cybersikkerhed

Juli 2017

CENTER FOR CYBERSIKKERHED

Dato: 7. juli 2017

Trusselsvurdering: DDoS-angreb stiger i antal og størrelse

Formålet med vurderingen er, at informere beslutningstagere om truslen fra Distributed Denial of Service angreb (DDoS), så den kan medtages i myndigheders og virksomheders risikovurdering. DDoS-angreb udgør en væsentlig trussel mod især online tjenester og kan true samfundsvigtige funktioner.

Hovedvurdering

- CFCS vurderer, at antallet af DDoS-angreb er stigende, og særligt hyppigheden og størrelsen af de kraftige angreb er øget.
- DDoS-angreb er målrettede. Derfor vil nogle organisationer sjældent eller aldrig blive ramt af DDoS-angreb, mens andre vil blive ramt regelmæssigt. Der er dog en risiko for at blive påvirket af følgevirkningerne af et kraftigt DDoS-angreb, selvom angrebet ikke er rettet direkte imod brugeren selv.
- CFCS vurderer, at selv et koordineret DDoS-angreb mod samfundsvigtige funktioner i Danmark vil kunne imødegås, således at disse funktioner kan opretholdes eller genskabes indenfor et døgn.
- DDoS-angreb er et værktøj som benyttes af flere typer cyberaktører. Angrebene kan ramme alle, som har en synlig IP-adresse på internettet. Truslen er dog særlig alvorlig for myndigheder og virksomheder, som leverer online tjenester eller sælger varer på internettet.
- Cyberkriminelle udgør en alvorlig DDoS-trussel. De benytter primært DDoS-angreb mod private virksomheder, med det formål at opnå en økonomisk gevinst.
- CFCS vurderer, at de fleste DDoS-angreb udføres af enkeltpersoner hvor formålet primært er spænding eller chikane. Selvom de fleste angreb er små og ikke truer samfundsvigtige funktioner, så findes der i denne gruppe også aktører, som er i stand til at udføre eller købe kraftige DDoS-angreb.

Analyse

Denne trusselsvurdering beskriver truslen fra Distributed Denial of Service angreb (DDoS), også kaldet overbelastningsangreb.

DDoS-angrebstyper

Volumen-angreb overbelaster kapaciteten (båndbredden) på internetforbindelsen.

Protokol-angreb overbelaster kapaciteten på en firewall, router eller anden netværkskomponent.

Applikations-angreb udnytter svagheder i programmerne på en netværkskomponent, f.eks. en webserver.

Alle virksomheder, myndigheder, organisationer eller borgere, som benytter en IP-adresse, der er synlig på internettet kan rammes af et DDoS-angreb. Angrebene udføres via internettet ved at sende så store mængder datatrafik mod en IP-adresse, at den bagvedliggende hjemmeside, onlinetjeneste eller netværkskomponent bliver overbelastet og derved utilgængelig for brugerne. Traditionel it-beskyttelse som antivirus-software og regelmæssig sikkerhedsopdatering af software beskytter ikke mod DDoS-angreb.

Omfanget af DDoS-angreb er vanskeligt at bestemme, og der findes ingen samlet og uafhængig statistik over antallet af angreb. Tal fra en førende udbyder af DDoS-beskyttelse indikerer imidlertid, at der i 2016 blev udført over 18 millioner DDoS-angreb globalt set. Tallet er behæftet med usikkerhed, fordi mange DDoS-angreb ikke registreres, og fordi statistikken kun er baseret på analyse af en del af datatrafikken på internettet. Imidlertid viser det, at DDoS-angreb sker hyppigt, og udgør en reel cybertrussel.

I modsætning til mange andre cybertrusler, er DDoS-angreb målrettede, hvilket betyder, at nogle organisationer sjældent eller aldrig vil opleve et DDoS-angreb, mens andre vil blive ramt af DDoS-angreb regelmæssigt. Enhver bruger af internettet risikerer dog at blive påvirket af følgevirkningerne af et kraftigt DDoS-angreb, selvom angrebet ikke er rettet direkte imod brugeren selv.

Et kraftigt DDoS-angreb mod f.eks. en hjemmeside kan medføre, at brugere, som befinder sig på samme it-infrastruktur som den angrebne hjemmeside, også oplever, at deres it-system ikke kan tilgås via internettet. Det kan for eksempel ske, hvis en kunde hos en hostingudbyder bliver udsat for et DDoS-angreb, som er så kraftigt, at udbyderens netværk bliver overbelastet, så andre kunders hjemmesider også bliver umulige at nå fra internettet. Den samme problematik gælder for internetudbydere og udbydere af cloud-løsninger, hvor flere kunder deler den samme infrastruktur. Derfor er DDoS-truslen særlig alvorlig for denne type virksomheder.

Et meget kraftigt DDoS-angreb kan også lamme eller forstyrre centrale services eller transmissionssystemer på internettet, og derved have negative konsekvenser for mange myndigheder, virksomheder og private borgeres adgang til internettet.

Et eksempel på et meget kraftigt DDoS-angreb, var angrebet i oktober 2016, mod en amerikanske udbyder af DNS-services (DYN). Angrebet bevirkede, at blandt andet brugere på den amerikanske østkyst, som blev serviceret af de angrebne DNS-servere, mistede adgangen til mange populære hjemmesider og tjenester, herunder Amazon, Twitter og Spotify. Angrebet bestod af flere separate DDoS-angreb, som toppede med en båndbredde på omkring 1000 Gbit/s.

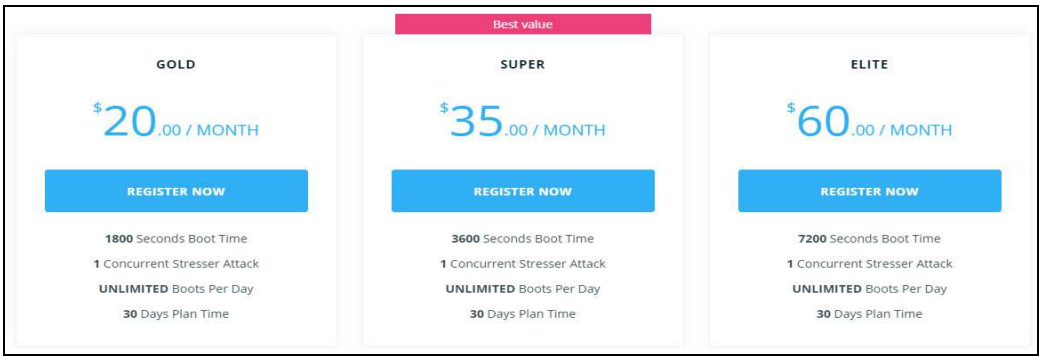
DNS-server
En internetservice som oversætter navne på hjemmesider til de IP-adresser, som netværkskomponenter benytter til at rute datatrafikken på internettet. Lokale computere og netværk indeholder DNS-servere med IP-adresser til tidligere besøgte hjemmesider. Hvis en lokal DNS-server ikke indeholder adressen til en hjemmeside, vil den spørge en central såkaldt autoritativ DNS-server. Hvis den centrale DNS-server ikke er tilgængelig, f.eks. på grund at et DDoS-angreb, kan computeren ikke etablere adgang til hjemmesiden.

Danmark er et højt digitaliseret samfund, hvor mange samfundsvigtige funktioner kræver en stabil internetforbindelse, ligesom mange virksomheder er afhængige af at kunne sælge deres produkter og levere deres services via internettet. Nogle eksempler er myndigheders borgerservice, som i dag i stor grad foregår via internettet samt udbydere af internettjenester, netbanker, webbutikker, sociale medier, nyhedsmedier og streaming af radio og TV. DDoS-angreb kan gøre disse online tjenester midlertidigt utilgængelige for brugerne, og medføre økonomiske tab for virksomhederne på grund af tabt omsætning og tab af kunder, og kan i sidste ende skade samfundet. Alene truslen for DDoS-angreb medfører øgede omkostninger for de organisationer, som ser sig nødsaget til at købe ekstra netværkskapacitet eller DDoS-beskyttelse.

En årsag til den høje forekomst af DDoS-angreb er, at simple angreb er lette at udføre ved hjælp af værktøjer som er tilgængelige via internettet.

Figur 1. Eksempel på DDoS værktøj til Android som kan downloades via Google Play

En anden årsag er, at DDoS-angreb udbydes som såkaldte ”Booter” eller ”stresser” -services via hjemmesider på internettet.



Figur 2. Prisliste på internettet for Booter tjenesten "Insta Booter"

Udover at give netværksejere mulighed for at teste deres eget netværks robusthed overfor DDoS-angreb, så er tjenesterne også tilgængelige for enhver som ønsker at udføre et DDoS-angreb mod en specifik IP-adresse. DDoS-angreb kan købes anonymt, ligesom disse hjemmesider ofte tilbyder mindre "test" DDoS-angreb gratis.

I en doktorafhandling fra George Mason universitetet i USA, blev det i 2016 påvist, at alene tre af disse Booter tjenester havde genereret mere end 600.000 DDoS-angreb over en periode på ca. 3 år.

Selvom simple DDoS-angreb er lette at udføre, så kræver et kraftigt DDoS-angreb mange ressourcer i form af infrastruktur/angrebskapacitet eller penge. Da cyberaktører typisk har begrænsede ressourcer, og ikke råder over eget botnet, som er i stand til at generere kraftige DDoS-angreb mod flere mål samtidig, så vil et DDoS-angreb altid være tidsbegrænset. Varigheden af et DDoS-angreb har holdt sig nogenlunde konstant indenfor de seneste år. Omkring 85 procent af alle registrerede DDoS-angreb varer under 30 minutter, og under én procent varer mere end et døgn.

Et alvorligt DDoS-angreb vil imidlertid ofte bestå af en række separate angreb som varierer i type, intensitet og varighed. Et DDoS-angreb kan altså betyde, at flere angreb er forestående. Hvis det første angreb ikke var effektivt, så er der yderligere en risiko for, at de efterfølgende angreb vil stige i intensitet. Denne angrebsmetode gør det vanskeligt, selv med DDoS-beskyttelse, at afværge et DDoS-angreb effektivt. Det gælder især hvis DDoS-beskyttelsen manuelt skal tilpasses, aktiveres og deaktiveres for hvert angreb.

Botnet
Et netværk af computere, routere, smartphones, og andre internetforbundne enheder, som indeholder applikationer eller malware, der gør det muligt at fjernstyre enhederne, således at de kan indgå i et koordineret DDoS-angreb.

Trusselsaktørerne og deres mål

DDoS-angreb er et værktøj, som benyttes af flere typer trusselsaktører, hvilket er en medvirkende årsag til at de er så udbredte.

Cyberkriminelle benytter DDoS-angreb for at opnå en økonomisk gevinst

Cyberkriminelle kræver penge for at stoppe et DDoS-angreb, eller benytter DDoS-angreb for at sløre et mere alvorligt cyberangreb. Nogle cyberkriminelle udbyder booter-tjenester mod betaling eller benytter botnet til at generere DDoS-angreb, som er så kraftige, at de kan forstyrre selv virksomheder med stor netværkskapacitet. De cyberkriminelle aktører udfører især DDoS-angreb mod private online virksomheder. Disse virksomheder er økonomisk sårbare overfor DDoS-angreb, og kan være mere tilbøjelige til at betale for at få stoppet et angreb.

I december 2015 optrevlede Europol i samarbejde med en række lande en cyberkriminel gruppe DD4BC (DDoS for Bitcoin) i Bosnien-Hercegovina. Gruppen havde specialiseret sig i at udføre DDoS-angreb mod især finansielle institutioner og udbydere af online spil. Angrebet ville stoppe, hvis offeret betalte en sum i Bitcoins. De registrerede angreb blev udført med en båndbredde, som var tilpasset til at kunne forstyrre eller lamme adgangen til den enkelte virksomheds hjemmeside. De fleste angreb var på 4-30 Gbit/s, men ifølge den nationale schweiziske CERT var gruppen i stand til at udføre angreb på helt op til 500 Gbit/s, hvis det blev nødvendigt for at lamme en virksomhed, som var særlig robust.

En anden gruppe som blev optrevlet i 2015 var "Lizard Squad". Gruppen drev og benyttede selv, DDoS-tjenesten "Lizard Stresser". Lizard Stresser blev angiveligt hacket i januar 2015, og lækkede data afslørede senere, at tjenesten havde ca. 13.000 brugere. CFCS har analyseret lækket, som også viser, at flere af de angrebne IP-adresser tilhører danske tele- og hostingudbydere.

De fleste DDoS-angreb udføres af enkeltpersoner, hvor formålet er spænding eller chikane

CFCS vurderer, at de fleste DDoS-angreb udføres af personer uden et politisk eller økonomisk sigte, og hvor det primære formål er spænding eller chikane. Disse personer får blandt andet deres viden fra en bred vifte af chatforums, hvor de deler erfaringer, køber og sælger hackerydelser eller hjælper hinanden med at hacke eller udføre DDoS-angreb. Det danske hackerforum shellsec.pw har i øjeblikket over 1700 medlemmer, og indeholder adskillige chattråde om DDoS. CFCS vurderer, at selvom de fleste angreb fra denne aktørgruppe er små og ikke truer samfundsvigtige funktioner, så findes der i denne gruppe også aktører, som er i stand til at udføre eller købe kraftige DDoS-angreb.

I gruppen af enkeltpersoner er også brugere af online computerspil. Indenfor gaming-verdenen er brugen af DDoS-angreb ganske udbredt. Dette kan skyldes, at en del gamere lægger mange følelser i deres hobby. Da mange engagerede spillere samtidig har god viden om den netværks- og computerteknik der bruges til computerspil, er der ikke langt fra aggression til at udføre DDoS-angreb mod en spiludbyder, spilserver eller modstander for at chikanere eller opnå en fordel i spillet. CFCS vurderer, at brugere og udbydere af online computerspil er særligt udsatte for DDoS-angreb.

Cyberaktivister benytter også DDoS-angreb, men omfanget er begrænset

Cyberaktivister fokuserer på enkeltsager, og benytter blandt andet DDoS-angreb mod myndigheder og virksomheder, som de opfatter som modstandere af deres sag. Et eksempel er hackergruppen Anonymous, som i 2010 gennemførte DDoS-angreb mod finansielle virksomheder, som nægtede at håndtere betalinger til WikiLeaks, og i 2012 udsatte svenske myndigheder for DDoS-angreb i protest over samme myndigheders razzia mod en virksomhed, som hostede fildelingstjenesten Pirate Bay og WikiLeaks. Islandske myndigheder og virksomheder er flere gange siden starten af 2016 blevet udsat for DDoS-angreb fra Anonymous operationen OpKillingBay. Angrebene er sket i protest mod Islands hvalfangst, og det vil derfor ikke være overraskende, hvis gruppen på baggrund af den grønlandske eller færøske hvalfangst, også vælger at angribe danske mål. Generelt er der dog ikke konstateret mange eksempler på cyberaktivisme i Danmark, men truslen vil stige, hvis en organisation forbindes med en sag, som har cyberaktivisternes opmærksomhed.

Omfanget og effekten af DDoS-angreb som er relateret til terrorisme er begrænset

Hackere som sympatiserer med terrororganisationer planlægger og udfører også DDoS-angreb. Formålet er at skabe opmærksomhed på terrororganisationerne og deres mål, for derved at skræmme befolkningen. Effekten af disse angreb har dog hidtil været begrænset, og CFCS har ikke kendskab til DDoS-angreb i Danmark, som kan tilskrives terrorgrupper eller hackere som sympatiserer med disse. En sandsynlig årsag er, at hackere som sympatiserer med terrorgrupperne ikke har kapacitet til at udføre effektive DDoS-angreb mod samfundsvigtige systemer, samt at de traditionelle terrorgrupper ikke ser DDoS-angreb som et effektivt middel til at nå deres mål.

DDoS-angreb kan også benyttes af stater og statsstøttede grupper

En række lande opbygger offensive cyberkapaciteter, og en af disse kapaciteter kan være DDoS-angreb. DDoS-angreb kan anvendes i forbindelse med en konflikt til at afbryde eller forstyrre samfundsvigtige funktioner i et land, men kan også anvendes politisk for at understrege et budskab eller påvirke meningsdannelsen i et land, f.eks. ved at lamme visse medier og hjemmesider eller ved at forstyrre en folkeafstemning. Motivet for et sådan DDoS-angreb kan sløres ved at udføre angrebet under dække af cyberkriminalitet eller cyberaktivisme.
Estland blev i 2007 over en periode på 3 uger udsat for et stort antal koordinerede DDoS-angreb, som især ramte landets myndigheder, medier og banker. DDoS-angrebet blev af Estland og flere medier tolket som en reaktion på Estlands fjernelse af et Russisk krigsmindesmærke.
Kina er kendt for at regulere indbyggernes adgang til internettet, ved at blokere for adgangen til udvalgte internettjenester, nyhedstjenester og sociale medier som for eksempel Facebook. Internettjenester som hjælper med at omgå denne blokering, er flere gange blevet udsat for DDoS-angreb. Flere offentlige medier spekulerer i, at nogle af disse DDoS-angreb kan være iværksat af kinesiske myndigheder. Eksempelvis blev organisationen Greatfire.org, som beskæftiger sig med internetcensuren i Kina, i marts 2015 udsat for et kraftigt DDoS-angreb som ifølge tekniske analyser så ud til at stamme fra Kina. Analysen af angrebet påviste dog ikke, at kinesiske myndigheder var involveret i angrebet.

En virksomhed kan benytte DDoS-angreb for at skade en konkurrent

Virksomheder eller personer, som er tilknyttet en virksomhed, som sælger varer, ydelser eller online tjenester via internettet, kan vælge at udføre DDoS-angreb mod konkurrenter for at skade konkurrentens økonomi og omdømme, og trække kunder over til egen virksomhed. CFCS har kendskab til, at denne form for chikane forekommer i Danmark, men kender ikke det konkrete omfang.

DDoS-angreb og deres effekt

De fleste små og mellemstore virksomheder i Danmark har internetforbindelser med en båndbredde under 50 Mbit/s, og selv større virksomheder har ofte forbindelser under 1 Gbit/s. I 2016 rapporter fra udbydere af DDoS-beskyttelse, varierer andelen af registrerede DDoS-angreb over 1 Gbit/s fra 20 procent til over 80 procent af det samlede antal angreb. Selvom disse tal er meget svingende, vurderer CFCS, at en væsentlig andel af det totale antal DDoS-angreb kan påvirke selv større virksomheder i Danmark.

Internetudbyder
Tilbyder internetforbindelser til kunder, typisk via fastnet eller mobilnet.

Hostingudbyder
Typisk en virksomhed som tilbyder den it-infrastruktur, og de it-værktøjer, som er nødvendige for at kunne oprette en hjemmeside og forbinde den til internettet. Kunden administrerer sin hjemmeside via internettet.

Cloududbyder
En virksomhed som via egen it-infrastruktur tilbyder it-services til kunder, som har adgang til disse services via internettet. Produkterne kan strække sig fra adgang til virtuelle servere eller softwarepakker som Microsoft Office til etablering og drift af avancerede it-løsninger.

Virksomheder som internetudbydere og udbydere af hosting- og cloudtjenester er særlig udsat for DDoS-truslen, da alle angreb mod deres kunder går via deres it-infrastruktur. Disse udbydere har imidlertid ofte stor båndbredde til rådighed, og kan derfor modstå større DDoS-angreb. CFCS vurderer dog, at et DDoS-angreb på 10 Gbit/s eller mere kan være en udfordring for flere danske udbydere. Andelen af registrerede DDoS-angreb over 10 Gbit/s varierer meget i forskellige offentliggjorte DDoS-rapporter for 2016. CFCS vurderer, at omkring 1 procent af det samlede antal DDoS-angreb oversteg 10 Gbit/s. Imidlertid er trenden stigende for de kraftige DDoS-angreb, hvorfor vi i fremtiden vil se en større andel af DDoS-angreb over 10 Gbit/s.

Et effektivt DDoS-angreb mod en myndigheds eller virksomheds hjemmeside kan, udover at lamme hjemmesiden, også betyde, at hele det netværk hvori webserveren er placeret, mister muligheden for at kommunikere via internettet. Det kan ske hvis en router eller firewall, som håndterer internettrafik til og fra netværket, bliver overbelastet, eller hvis de såkaldte ”handshakes” som er nødvendige, for at virksomheden kan etablere en dataforbindelse via internettet, ikke kan modtages på grund af DDoS-angrebet. Et effektivt DDoS-angreb kan derfor, udover at påvirke tilgængeligheden af en hjemmeside, også påvirke andre tjenester som kræver en fungerende internetforbindelse. Disse tjenester kan for eksempel være IP-telefoni, e-mail eller adgangen til eksterne cloud-løsninger.

Mobilnettene benyttes i dag overvejende til datatrafik til og fra internettet. Simple DDoS-angreb kan udføres via apps på smartphones, og mobile enheder kan indgå i botnet, ligesom der kan udføres DDoS-angreb mod infrastrukturen i mobilnettene. Der har både i Danmark og i udlandet været eksempler på DDoS-angreb rettet imod infrastruktur i et mobilnet, som har betydet, at dele af mobiltjenesterne i en periode ikke har været tilgængelige for slutbrugerne.

Afværgelsen af et DDoS-angreb kan spærre for legitim datatrafik. Hvis en kunde hos en udbyder af internettjenester udsættes for et alvorligt DDoS-angreb, kan udbyderen vælge at beskytte sit netværk og øvrige kunder ved at blokere for al datatrafik til den angrebne kunde, eller at blokere for al datatrafik fra de IP-adresser eller geografiske områder, som angrebet kommer fra. Førstnævnte metode har den uheldige konsekvens, at den forstærker angrebets effekt set fra kundens side, og geoblokering kan medføre, at der også spærres for legitim datatrafik fra det blokerede område, hvilket kan have negative konsekvenser for de af udbyderens kunder, som har infrastruktur, kontorer, underleverandører eller egne kunder i de lande eller områder som bliver geoblokeret.

Danmarks it-infrastruktur er generelt robust overfor DDoS-angreb

Et kraftigt og koordineret DDoS-angreb mod internettet i Danmark kan give alvorlige forstyrrelser, særligt i de første timer af angrebet. CFCS vurderer imidlertid, at internetudbyderne i Danmark vil være i stand til at afbøde og inddæmme et sådan angreb, således at samfundsvigtige funktioner kan opretholdes eller genskabes indenfor et døgn.

Det tidligere omtalte DDoS-angreb mod Estland i 2007, kan tolkes som et forsøg på at lamme landets internet, og i november 2016 blev Liberia udsat for et DDoS-angreb, som påvirkede en stor del af landet internetbrugere. Estland var i stand til, at afbøde virkningerne af angrebet, blandt andet ved anvendelse af de tidligere omtalte metoder, hvilket i høj grad også vil være muligt i Danmark. Årsagen til at effekten af angrebet på Liberia blev så stor, var at størstedelen af internettrafikken til Liberia gik via en enkelt forbindelse. Internettet i Danmark er imidlertid forbundet til udlandet via flere land- og søkabler.

Et DDoS-angreb på hele Danmarks internet, kan søge at overbelaste de største internetudbyderes netværk, så disse netværk overbelastes, og ikke har kapacitet til at route datatrafik til de underliggende netværk. Et koordineret DDoS-angreb kan også rettes imod samfundsvigtige hjemmesider og online tjenester. Endelig kan en angriber forsøge at overbelaste de autoritative DNS-servere, som håndterer "adressebogen" for alle hjemmesider med navne som ender på ".dk". Disse netværk og servere har imidlertid stor netværkskapacitet, og anvender ofte flere forskellige former for DDoS-beskyttelse, som betyder, at de er robuste og kan håndtere eller filtrere store DDoS-angreb mod dem selv eller deres kunder.

En udfordring i forbindelse med afværgelsen et kraftigt og koordineret DDoS-angreb mod Danmark vil være de administrative og praktiske udfordringer når myndigheder og administratorer

af de netværk, som udgør internettet i Danmark, skal erkende angrebet og koordinere modforanstaltningerne. Derfor vil konsekvenserne af et sådan angreb være særligt store i det første døgn, hvor beredskabet endnu ikke er fuldt aktiveret.

Den fremadrettede DDoS-trussel

Antallet af DDoS-angreb stiger, og hyppigheden og størrelsen af de kraftige angreb er stigende. Siden 2013 er der sket en markant stigning i båndbredden af de kraftigste registrerede DDoS-angreb, således at disse nu kan være på flere hundrede Gbit/s, og har nået en størrelse, som kan true kapaciteten af centrale internetservices og de største internetudbyderes netværk. En global udbyder af DDoS-beskyttelse registrerede det første angreb over 100 Gbit/s i 2013, og siden er antallet af angreb steget til mere end 500 i 2016. Selvom angreb over 100 Gbit/s stadig er relativt sjældne sammenlignet med det samlede antal DDoS-angreb, så forekommer de også i Danmark. CFCS vurderer, at den stigende tendens vil fortsætte.

Internet of Things kan medvirke til en fortsat stigning i hyppigheden af kraftigere DDoS-angreb

En medvirkende årsag til stigningen i hyppigheden og størrelsen af de kraftigste angreb er, at flere og flere produkter så som køleskabe og babyalarmer forbindes til internettet, en udvikling som kaldes Internet of Things (IoT). Når flere enheder forbindes til internettet, vil der uværligt være nogle af disse enheder, som indeholder sårbarheder, der kan udnyttes til DDoS-angreb. Risikoen er særlig stor, hvis enheden er fremstillet af en producent, som ikke prioriterer, eller som ikke har erfaring med, at tænke cybersikkerhed ind i de internetforbundne produkter. Endvidere vil mange af fremtidens IoT-enheder formentlig aldrig modtage sikkerhedsopdateringer, som kan fjerne eventuelle sårbarheder.

Det tidligere omtalte DDoS-angreb mod DYN i oktober 2016, anvendte netop et botnet bestående af kompromitterede IoT-enheder, til at generere en angrebstrafik på op til 1000 Gbit/s.

Ifølge Ericsson Mobility Report fra november 2016, er der i dag over 5 milliarder IoT-enheder som er forbundet til internettet, og Ericsson forventer, at tallet vil være steget til 18 milliarder i 2021. En sandsynlig konsekvens af denne stigning vil være, at antallet og størrelsen af de kraftigste DDoS-angreb vil vedblive at stige.

IoT har betydet, at en række nye netværksteknologier har set dagens lys. Nogle eksempler er Narrowband IoT, som bygger på de eksisterende 4G mobilnet, LoRa som er en form for Wi-Fi netværk og det nye landsdækkende SigFox-netværk. Disse typer netværk er enten allerede i drift i Danmark eller er ved at blive etableret. Fælles for disse nye netværk gælder det, at de alle har forbindelse til internettet, hvorfor de potentielt kan indgå i et DDoS-angreb. For LoRa og i særdeleshed SigFox gælder det dog, at netværkene har så lille datakapacitet, at de sandsynligvis ikke vil kunne anvendes til DDoS-angreb. Imidlertid kan de nye netværk selv blive mål for DDoS-angreb, hvor den lave datakapacitet gør dem sårbare.

Åbne services i netværksudstyr vil fortsat muliggøre amplification-angreb

Omkring halvdelen af alle registrerede volumen-angreb udføres som såkaldte amplification-angreb. Amplification-angreb er mulige, fordi mange internetbrugeres netværksudstyr indeholder såkaldte åbne services, som besvarer alle forespørgsler fra enhver computer på internettet. Da ejeren af netværksudstyret typisk ikke selv oplever problemer, hvis udstyret udnyttes i et DDoS-angreb, er der et begrænset incitament for ejeren til at tjekke og sikre dette netværksudstyr. DNS-servere bliver ofte brugt i amplification-angreb. På hjemmesiden openresolverproject.org kan man se, at der i januar 2017 var over 10 millioner åbne DNS-servere på internettet. Selvom antallet er reduceret fra godt 20 millioner i 2013, så vurderer CFCS, at det samlede antal åbne services på internettet er så stort, at truslen fra amplification-angreb vil være uændret på mellemlangt sigt.

Amplification-angreb

Betegner volumen-angreb som forstærkes ved at udnytte, at visse internetservices kan generere en stor mængde datatrafik som svar på forespørgsler, der kun kræver en lille mængde datatrafik. En angriber kan forfalske IP-adressen på tusindevis af sådanne forespørgsler således, at de mange og datatunge svar rammer den IP-adresse eller hjemmeside som angriberen ønsker at lamme.

Øget digitalisering og centralisering af datatjenester kan øge effekten af fremtidige DDoS-angreb

Den øgede digitalisering af samfundet øger myndigheders, virksomheders og borgeres afhængighed af online tjenester, som udbydes over internettet. I takt med at områder som sundhedsvæsen, renovation, gadebelysning, forsyning, indeklima, transport og lignende i stigende grad kobles til internettet, kan et DDoS-angreb mod disse funktioner få negative konsekvenser for samfundsvigtige funktioner.

Flere og flere myndigheder og virksomheder benytter sig af såkaldt Cloud Computing, som gør det muligt at flytte data, it-infrastruktur eller online-tjenester ud i centrale datacentre. Den stigende brug af cloud-løsninger kan derved medføre en øget centralisering af samfundsvigtig it-infrastruktur og data. Hvis en cloud-løsning er forbundet via internettet, øges også afhængigheden af stabile internetforbindelser. Et effektivt DDoS-angreb mod en cloud-løsning eller udbyder af Cloud Computing kan ramme flere myndigheder eller virksomheder samtidigt, og derved få alvorlige konsekvenser for samfundet.

Anbefalinger

CFCS anbefaler alle virksomheder og myndigheder, at inddrage DDoS-truslen i organisationens risikovurdering. I forbindelse med risikovurderingen er det vigtigt også at inddrage DDoS-truslen mod underleverandører. Dette gælder især hvis kritiske dele af forretningen er placeret ved en hosting- eller cloududbyder.

CFCS har udarbejdet flere vejledninger om DDoS-truslen:

- **Sådan kan du imødegå DDoS-angreb**
  Anbefalinger som øger myndigheders og virksomheders robusthed overfor DDoS-angreb.

- **Undgå DNS amplification attacks**
  Vejledning i hvorledes netværksadministratorer kan finde og sikre åbne DNS-servere, som kan misbruges i et amplification-angreb.
- **SNMP Reflected Amplification DDoS-attacks**
  Vejledning i hvorledes netværksadministratorer kan finde og sikre åbne SNMP-services, som kan misbruges i et amplification-angreb.

Udover DNS og SNMP er der en række andre netværksservices, som også kan udnyttes i et amplification-angreb. CFCS anbefaler alle virksomheder og myndigheder til at orientere sig om emnet, og undersøge om deres it-infrastruktur indeholder åbne services, som bør konfigureres til kun at acceptere forespørgsler fra bestemte IP-adresser.

Forfalskning af IP-afsenderadressen er en forudsætning for at kunne lave amplification-angreb. Forfalskningen gør det samtidigt vanskeligt at imødegå et DDoS-angreb, da angrebets oprindelse sløres. CFCS anbefaler internetudbydere og andre virksomheder, som administrerer en del af internettets IP-adresser til at implementere standarden BCP38. Standarden indeholder anbefalinger til netværkskonfiguration, der imødegår muligheden for, at IP-pakker med falsk afsenderadresse kan forlade netværket. Yderligere information om BCP38 kan findes på internettet.

FE bruger denne skala for sandsynlighed i analyser: