Säkerhet på Internet – datavirus och blockering av tjänster

Observatoriet för informationssäkerhet Observatorierapport 23/2000

Förord

Säkerhet när det gäller IT-området är inte någon ny företeelse, men det har blivit ett växande problem i takt med den ökade anslutningen till Internet, framför allt genom det växande antalet fasta anslutningar med hög kapacitet, det som i dagligt tal benämns som bredbandsanslutningar.

Det finns en stor mängd faror på Internet. Precis som i andra situationer finns det dock olika verktyg och metoder för att undvika eller mildra effekten av dessa faror. För att veta vad vi ska skydda oss mot är det alltid bra att veta vilka hot[1] som existerar. Denna rapport diskuterar några av de vanligaste hoten - datavirus och blockering av tjänster. Hot som följer med anslutning till Internet.

Kontaktperson för rapporten och för IT-kommissionens arbete med informationssäkerhet är Anne-Marie Eklund Löwinder, IT-kommissionen.
E-post: anne-marie.eklund-lowinder@itkommissionen.se

Stockholm november 2000-11-06

Hans Wallberg
Ordförande observatoriet för

Christer Marking
Kanslichef för IT- informationssäkerhet kommissionen

[1] Ett hot definieras som en möjlig, oönskad händelse som ger negativa konsekvenser för någon. Risk är sannolikheten för att en oönskad händelse skall inträffa. Dvs. det faktum att det finns ett hot innebär inte med automatik att man behöver drabbas av det. Utgående från en riskbedömning kan man anpassa skyddet.

Inledning

I och med den ökade användningen av datorer i hemmen har riskerna flyttats något. Det är ofta så att datorn hemma också används för att arbeta hemifrån. Skyddet av hemdatorer är ofta sämre än skyddet av datorerna på våra arbetsplatser. Detta kan leda till konsekvenser inte minst för arbetsgivaren.

Det vanliga är att våra datorer kan bli infekterade av virus och att någon kan göra intrång i dem, med eller utan vår vetskap, och därigenom få tillgång till eller ändra vår lagrade information. Beroende på vilken programvara och vilka tjänster vi använder vår anslutning till Internet för, finns olika risker att den egna informationen görs tillgänglig från andra. Det finns också exempel där användare i kommunikation med andra (via e-post, icq, chat osv.) uppmanas att utföra kommandon på den egna maskinen som skapar möjligheter att komma åt information utifrån, köra program eller till och med förstör datorn, raderar information etc.

Datavirus

Mängden datavirus[2] ökar i en oförutsägbar takt. Om vi startar från 1986 så fanns då endast ett känt datavirus. Tre år senare hade antalet ökat till sex, och 1990 fanns totalt 80 kända virus. I november samma år upptäcktes nya datavirus i en takt med ett nytt virus per vecka. Från december 1998 till oktober 1999 tog mängden upptäckta virus ett skutt från 20 500 till 42 000. I nuläget säger statistiken att man upptäcker mellan 10 och 15 nya virus dagligen. Ett par hundra virus betraktas som mycket spridda (in the wild).

Enligt International Computer Security Association (ICSA), har disketter tidigare varit den vanligaste smittkällan, motsvarande 68 procent av alla rapporterade smittillfällen under 1998 och 38 procent 1999. Datavirus som sprids via e-post ökade under samma tid från 32 procent 1998 till 56 procent 1999. Bilagor till e-post är den vanligaste smittbäraren av makrovirus, medan disketter är den typiska bäraren av s.k. boot-sektorvirus.

Ett datavirus är en självständig del av ett program som kan döljas i ett annat program där virusprogrammets instruktioner inte utförs förrän det program där det ligger gömt aktiverats. Precis som ett biologiskt virus smittar det den miljö där det inplanterats genom att det kan kopiera sig själv till andra filer i omgivningen. Smittan fungerar tämligen enkelt. Viruset kan dessutom innehålla en s.k. logisk bomb som består av ett antal instruktioner (radera hårddisken, ta bort alla bilder etc.) som utförs när någon förutbestämd händelse inträffar, t.ex. vid en viss tidpunkt, ett visst datum eller liknande.

---

[2] Begreppet virus används ibland lite slarvigt. Det kan ibland vara viktigt att veta skillnaden mellan datavirus och andra obehagliga företeelser som existerar. En del av de saker som beskrivs som virus är i själva verket något annat, som förvisso inte behöver vara harmlöst utan som kan orsaka lika stor eller ännu större skada än ett virusangrepp.

När en användare hämtar eller får information utifrån kan denna vara bärare av virus i någon form. Det finns exempelvis makron, små kommandofiler, till Word och Excel som kan döljas i ett dokument, och som startar när dokumentet öppnas.

En trojansk häst är en dold, odokumenterad del av ett program. Denna dolda del kan innehålla en logisk bomb, ett virus eller någon annan sorts otrevlig programkod, och kan ibland till och med vara så konstruerat att det raderar ut sig själv för att sopa igen spåren när väl skadan är skedd.

Maskar, slutligen, är självständiga program, som alltså inte är beroende av att kunna döljas i ett annat program. Likt virus kopierar maskar kopierar sig själva och breder ut sig i hela nätverk, så fort som möjligt. Följden blir att tillgängligheten till datorerna minskar och ibland blir belastningen så stor att inga andra program kan fungera.

Vad man än kallar dessa saker så finns det inte några entydiga definitioner, och de är inte ömsesidigt uteslutande. Ett virus kan t.ex. innehålla en logisk bomb, en trojansk häst kan visa sig vara en mask etc. Många av de datavirus som sprids är också varianter av tidigare sorter.

Falska virus

Ett falskt virus, ett s.k. hoaxvirus är ett e-postmeddelande med avsikt att skrämma upp användare för att drabbas av ett icke-existerande virushot.

Titt som tätt får användare varningar via e-post från vänner och bekanta på Internet om att de ska se upp för ”farliga” e-post meddelanden med en viss rubrik, och som sägs innehålla ett virus som rensar hårddisken, förstör processorn eller liknande. Varningen går ut på att man inte ska läsa det om man får ett sådant meddelande med en angiven rubrik, utan bara ta bort det.

Gemensamt för den här typen av varningar är att man också uppmanas att sprida informationen till alla vänner och bekanta som använder e-post. Information om denna typ av meddelanden finns på många ställen på Internet. Ibland finns det dessutom en bilaga bifogad till meddelandet. Den bör man INTE öppna.

Många gånger går det mer tid åt att hantera denna typ av rykten än att hantera riktiga virusattacker. Att användare skickar varningar till varandra kors och tvärs genom nätet skapar mycket problem, inte bara trafikmässigt, utan också resursmässigt på en massa ställen runt om i världen, vilket i sin tur naturligtvis kostar en massa pengar. Därför bör man aldrig skicka denna typ av varningar vidare (trots att det står att man ska göra det). Inte utan att kontrollera närmare vad det är.

Det kan också vara bra att ta kontakt med källan till varningen och informera om hoaxvirus, var man kan hitta information om dessa, och hur man bör hantera dem. På det sättet kan alla medverka till att minska det resursslöseri som denna typ av varningar utgör.

Det finns några sätt att försöka identifiera falska virus. Dessa meddelanden är ofta formulerade med ett tekniskt vederhäftigt och välformulerat språk och det påstås ofta komma från etablerade och välkända organisationer som t.ex. Microsoft. Om varningen har den rätta tekniska jargongen har de

flesta människor en tendens att tro att varningen är riktig. Ofta finns det mycket versaler och utropstecken i texten. Särskilt misstänksam ska man vara mot virusvarningar som uppmanar en att vidarebefordra meddelandet till alla man känner. Bara detta borde föranleda en höjning av varningsflaggan för att det kan vara en hoax.

Vem tillverkar virus?

Virus tillverkas över hela världen. I princip kan vem som helst skriva ett virusprogram eftersom det på Internet finns tillgång till sådan information. Eftersom det inte är svårt att tillverka virus återfinns tillverkare av sådana i många olika sammanhang. Hackers, skolelever, någon som bara har tråkigt, någon som verkligen vill göra skada osv. Det finns inte skäl att utesluta någon i det sammanhanget.

Hur sprids datavirus?

Det existerar skillnader mellan de olika företeelserna när det gäller spridningssättet. I vissa fall, som när det gäller trojaner, måste den bli hämtad eller överlämnad av någon. Virus sprids oftast när man laddar hem program eller utbyter information (t.ex. bifogade filer i e-post). Maskar sänder iväg sig själva, via e-post, chatt eller liknande, och installerar också sig själv i mottagarens dator. Melissa och LoveLetter är exempel på detta.

Smittspridningen kan ske olika snabbt, beroende på vilken typ av program och datormiljö viruset har lagts in i och vilka egenskaper det för övrigt utrustats med. Vilken typ av skador ett datavirus förorsakar beror dels på vilka avsikter tillverkaren haft och dels på hur snabbt man upptäcker angreppet. Effekten kan variera från att åstadkomma en ”harmlös” utskrift på datorns skärm till att innehålla instruktioner som att förändra information (t.ex. slumpmässigt ändra värden i ett Excel-dokument), stjäl lösenord och ger andra tillträde till information eller förstöra all information som lagrats på hårddisken och dessutom skicka sig själv vidare till alla mottagare i den adressbok som finns i e-postprogrammet. De flesta virus som sprids gör emellertid inte någon skada över huvud taget. Bortsett från det irriterande faktum att man lägger ner en massa tid på att få bort det, harmlöst eller inte. I den meningen orsakar alla virus skada för de människor som drabbas av dem.

Det finns virus för alla operativsystem. Det finns också virus för alla vanligaste programmen. Det finns idag mer än 50 000 kända virus, och mängden ökar kontinuerligt. Stor risk att drabbas löper den som ofta byter program med andra och laddar ner program som man inte vet varifrån det kommer.

Hur upptäcker man virus?

Det finns olika sätt att upptäcka datavirus. Det absolut tråkigaste sättet är ju att upptäcka att man drabbats av ett. Vilket kan vara nog så svårt ibland. Oväntade utskrifter på skärmen, systemet går trögt, det tar längre tid än vanligt att starta dator eller program, program som ska finnas i systemet går inte att hitta, ledigt utrymme minskar drastiskt trots att man inte lagrat nämnvärda mängder,

okända filer dyker upp i programbiblioteket etc. är händelser som kan inträffa även om man *inte* drabbats av virus. Det vet alla som arbetat med datorer att de mest häpnadsväckande saker kan inträffa när man t.ex. installerat en ny version av en programvara.

Ett bra sätt att upptäcka virus är att använda ett antivirusprogram. Ett sådant reagerar och varnar vid förekomst av de virus som programmet kan känna igen. Det bästa är att prenumerera på uppdateringar av sitt virusprogram, med tanke på att det upptäcks flera hundra nya virus varje vecka, året om. För att få ett så bra skydd som möjligt är det viktigt att följa med och uppgradera det egna virusprogrammet så att också det känner till och klarar av att plocka bort de nyaste virusförekomsterna.

Hur kan man skydda sig mot datavirus?

Med tanke på att risken för att smittas av virus är överhängande, och med tanke på det besvär ett virus kan ställa till med så finns det goda skäl att vidta åtgärder för att förhindra att den egna datorn blir smittad.

När det gäller skydd är det fråga om

- att förebygga att man över huvud taget blir smittad
- att upptäcka ett virus och hindra smittspridning
- att återställa ett smittat system.

Det effektivaste är att undvika att bli smittad och det är därför främst de förebyggande åtgärderna som ska prioriteras. Men ibland hjälper inte det, och då måste man också ha en plan för hur man ska gå tillväga om olyckan skulle vara framme.

Förebyggande skydd

De förebyggande skydden är beroende av olika faktorer, t.ex. vilken datormiljö man har, vilken typ av anslutning som finns, vilken typ av program som körs osv. Det finns ett stort antal antivirusprogram på marknaden som kan användas. Många leverantörer av antivirusprogram ger ut nya versioner kontinuerligt, för att hålla takt med upptäckten av nya virus. Det är mycket viktigt att regelbundet uppdatera virusskyddet i den egna datorn.[3]

Några tumregler:

- Öppna inte bifogade filer eller program om du inte känner igen avsändaren eller som har underliga format som du inte känner igen.
- Se till att ha installerat och aktiverat ett virusskydd som uppdateras kontinuerligt.
- Ladda ner programfiler från mer kända webbplatser som kan förväntas ha en viss viruskontroll.

[3] http://www.symantec.se/avcenter/
Symantecs Antivirus Center är ett exempel där det går att finna aktuell och uppdaterad information om datavirus

?? Säkerhetskopiera regelbundet all information som du inte kan avvara. Skulle olyckan vara framme så är det enkelt att läsa tillbaka informationen när datorn är ”ren” igen.

Blockering av tjänster (Denial of Service)[4]

Ett annat problem som blivit vanligt på senare tid är när någon försöker sabotera genom att se till att vi inte kan nå ut till och använda nätet. Det enklaste sättet att åstadkomma det är att skicka en så stor mängd meningslös trafik över vår Internet-anslutning så att vår egen trafik inte kommer fram. Allt som krävs för detta är en Internet-anslutning med hög kapacitet, eller vissa tricks. Denna typ av attack kallas för 'Denial-of-Service' eftersom det är någon som genom sabotage ser till att vi inte får tillgång till en tjänst (Internet exempelvis).

Vad är en distribuerad denial-of-service-attack (ddos)? [5]

En ddos-attack behöver inte vara riktad mot någon enskild person utan det kan ofta finnas ett större intresse av att sabotera en handelsplats eller informationsplats. Eftersom dessa brukar ha anslutning med mycket hög kapacitet till Internet, så krävs det en attack från många olika punkter samtidigt för att det ska gå att fylla förbindelsen med inkommande trafik. Det är vad som har hänt i de fall mot Yahoo, CNN, m.fl. som det har skrivits om i pressen.

Hur genomförs en attack?

Enkelt uttryckt så skickar angriparen en så stor mängd meningslös trafik till offret så att offrets system blir översvämmat. Därmed kan offret inte ta emot några riktiga förfrågningar och andra på nätet upplever det som att de är borta. För att kunna slå ut ett stort offer som har anslutning med hög kapacitet till Internet så behövs det ett stort antal datorer som på ett koordinerat sätt skickar den meningslösa trafiken. För att kunna göra detta så använder sig den som vill utföra attacken sig av ett stort antal andra datorer, här kallade slavar. Dessa slavar är spridda över Internet och ägs av andra än angriparen. Han eller hon måste först ha gjort intrång i dem för att komma åt dem som resurs. I bilaga 1 beskrivs schematiskt hur en ddos-attack går till.

---

[4] Det finns inte någon bra svensk benämning av fenomentet ddos-attack. Vi har valt att kalla det blockering av tjänst.

[5] http://staff.washington.edu/dittrich/misc/ddos/
Här finns en lång lista med referenser till analyser av olika verktyg, olika papper och presentationer om ddos, verktyg för att upptäcka olika ddos-verktyg, m.m. av David Dittrich, en person som har lagt ner mycket arbete på att studera detta fenomen.

http://www.cert.org/advisories/CA-2000-01.html
CERT (Computing Emergency Response Team) är en organisation som övervakar säkerheten på Internet. De skriver rapporter om olika problem och fenomen som uppstår. Det här är en beskrivning av de ddos-attacker som har inträffat.

Det förberedande steget, att göra intrång i alla datorer som ska agera slavar, är i dagsläget alldeles för enkelt att genomföra eftersom alltför många datorer på Internet är tämligen oskyddade.

När angriparen väl har skaffat sig tillträde till ett stort antal datorer som kan användas vid attacken, så kan en ddos-attack startas med ett enda kommando, en tangenttryckning. Kommandot skickas ut från en dator (master) någonstans till alla dessa datorer som är slavar och beordrar dem att skicka stora mängder meningslös trafik till ett och samma offer. Om det går att få tillgång till tillräckligt många datorer med tillräckligt stor bandbredd så går det att slå ut även de allra största Webb-platserna.

Det är inte heller säkert att det är lätt för den som blir anfallen att skilja mellan legitim och meningslös trafik. Hur ska en webb-server kunna veta vilka frågor som kommer från riktiga användare och vilka som bara är skickade för att fylla förbindelsen? Det är i det generella fallet mycket svårt och även om vi idag kan känna igen vissa av de förekommande programmens genererade data så är det en smal sak för en person med blygsamma kunskaper att ändra dessa. Om vi hittar något sätt att skilja mellan onda och goda, då är det ofta för sent, förbindelsen är ju redan full med ”de ondas” trafik och den måste släppas fram innan det går att bedöma att vi inte vill ha med dem att göra.

Hur kan man spåra en attack?

För att ta reda på vem som ligger bakom en attack skulle vi behöva spåra all kommunikation baklänges tills vi hittar den som tryckte på tangenten för att utlösa den elektroniska flodvågen. Men den personen behöver inte ens sitta vid tangentbordet just då, utan kan ha förprogrammerat attacken. Om de slavar som användes för att skicka den stora mängden meningslös trafik aldrig används igen så bedömer vi chanserna att spåra ett steg till bakåt mycket små. Den försiktige angriparen kommer att använda sig av många flera datorer på vägen innan intrånget i slavarna sker, för att minska spårbarheten.

Det går inte alltid att lita på den information som finns tillgänglig om varifrån trafiken avsänts. Det är datorn som sänder datapaketen som är ansvarig för att stämpla in avsändare och mottagare. Om den som ligger bakom attacken har tagit full kontroll över datorn så kan avsändaradressen ändras till vad som helst. Det betyder att vi inte kan ta reda på vilka slavarna är eller veta vilken del av trafiken som vi inte vill ha med att göra och bör försöka slänga bort.

I många av de program som idag används för ddos-attacker så finns funktioner för att slumpmässigt tilldela avsändaradresser. Den enda som har en chans att veta om adresserna är korrekta är en avsändande dators anslutning till Internet. Den dator som agerar dörr i anslutningen känner till vilka adresser som sitter innanför den och ska ställas in så att den inte släpper ut några andra avsändaradresser än förväntade till Internet. Den mottagande datorns Internet-anslutning däremot inte någon möjlighet att veta att trafiken kom från en annan del av Internet än den påstår.

Vilka kan genomföra en attack?

Det borde ju vara mycket få personer i världen som både har tillräckliga kunskaper och den brist på etik och moral som krävs för att genomföra attackerna?

Att skriva program som kan göra en ddos-attack möjlig är inte svårt. Det finns ganska många som skulle klara av det och alltid kommer det finnas några av dem som inte tror, förstår eller vill förstå att det gör skada. Att dessutom modifiera ett befintligt program så att det gör något lite annorlunda eller elakare är mycket enkelt och kräver nästan inga kunskaper alls. Att kopiera programmet från någon annan och köra det kräver ungefär samma datorvana som vilken Internet-surfare som helst har. Svårigheten med att attackera en stor webbplats är att det kräver att man först kan göra intrång i en stor mängd datorer. Även om vi ovan säger att det är alltför lätt så kräver det trots allt en stor portion tålamod och relativt mycket mer kunskap än att bara klicka.

I nuläget har fem kända verktyg påträffats för den här typen av attacker. De har alla ett gemensamt ursprung och sprids likt sporer över Internet. De "trinoo", "Tribe Flood Network" (TFN), "stacheldraht", TFN2K och "shaft".

Vad kan vi göra för att försvara oss mot attacker?

Hur kan vi se till att detta inte händer oss? Och hur kan vi se till att detta inte är något problem?

Det första är att inse att alla sitter i samma båt och att det inte räcker med att lösa problemet i vår egen router, server eller dator[6]. Om alla andra datorer på nätet är osäkra så kan dessa användas som språngbrädor för en attack mot dig eller någon annan. Därför är vi alla beroende av varandra. Om alla har säkra datorer så kan vi inte bli drabbade av den här farsoten, åtminstone inte i lika stor skala. Det går inte att säga att jag inte har något viktigt på min dator - och att den därför inte behöver skyddas. Varje Internet-ansluten dator utgör ett vapen som någon annan kan gripa tag i och rikta mot någon tredje person.

För att minska riskerna för det här högst verkliga problemet, så behöver inte bara användarna, utan också de systemansvariga, återförsäljarna och leverantörerna vara med. System som säljs måste vara säkra i sitt grundutförande till en viss grundnivå. De allra flesta användare ändrar inte på några inställningar, åtminstone inte utan tydliga anvisningar. Det är naturligtvis vi som köper dessa system som ändå måste formulera och ställa dessa krav. Operatörerna måste vidta åtgärder i sina nät för att både detektera och göra det svårare att genomföra ddos-attacker och framför allt göra så att det går att spåra dem som ligger bakom attacken.

Det viktigaste vi kan göra nu är att se till att attacker kan spåras och att se till att våra datorer inte kan användas i en attack.

Skyddsåtgärder:

- säkra datorer

[6] http://www.ietf.org/rfc/rfc2644.txt
Ett dokument från IETF som beskriver hur man bör konfigurera system för att inte tillåta 'directed broadcast'.

- införa filtrering i routrar [7] [8] [9]
- ha sådan övervakning så att intrångsförsök och ddos-försök upptäcks
- tala med den egna operatören om vad de gör för att hindra problemet och hur man ska rapportera till dem när något händer[9]

---

[7] http://www.cert.org/reports/dsit_workshop.pdf

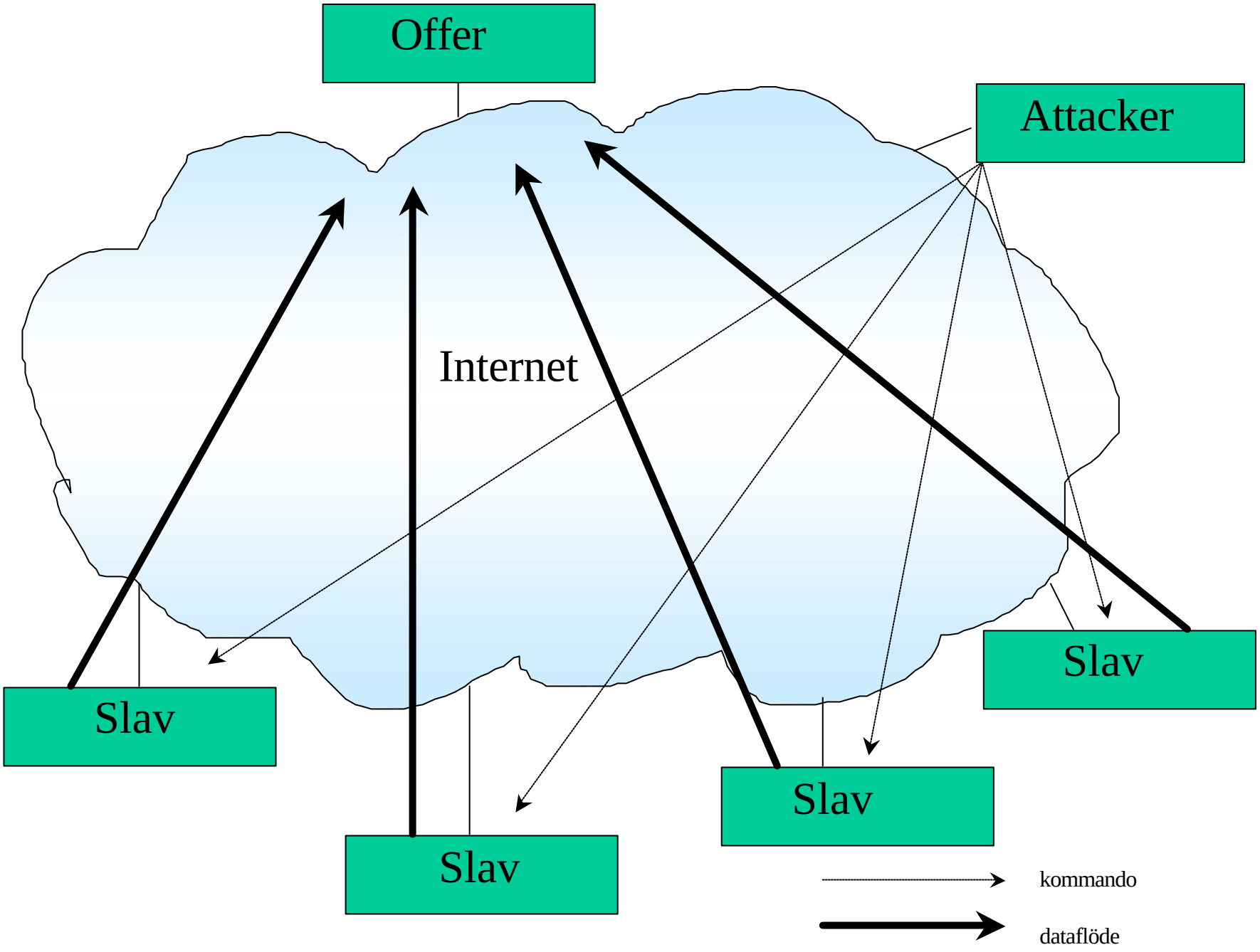
Rapport från Distributed-Systems Intruder Tools Workshop. En uppsättning folk från akademia och industrin som har skrivit ett dokument om problemet och vad som går att göra åt dem.

[8] http://www.cisco.com/warp/public/707/newsflash.html

Cisco (den största routertillverkaren) har publicerat en beskrivning av problemet och vad man kan göra med deras programvara.

[9] http://www.sans.org/dosstep/index.htm

En steg-för-steg beskrivning av SANS (System Administration, Networking, and Security) över hur du kan försvåra genomförandet av ddos-attacker.


Offer
Attacker
Internet
Slav
Slav
Slav
Slav
kommando
dataflöde