Rapportnummer PTS-ER-2009:11
Datum 2009-03-11

Botnät

Kapade datorer i Sverige

Botnät
Kapade datorer i Sverige

Rapportnummer
PTS-ER-2009:11

Diarienummer
08-10634

ISSN
1650-9862

Författare
Rapporten är sammanställd av en projektgrupp ledd av Per Bergstrand. I arbetet har Kristian Borryd, Staffan Lindmark och Adolf Slama deltagit.

Post- och telestyrelsen
Box 5398
102 49 Stockholm
08-678 55 00
pts@pts.se
www.pts.se

Förord

I takt med att Internets betydelse i samhället växer och såväl näringsliv som den breda allmänheten blir allt mer beroende av tillgång till Internet med god funktion och hög kapacitet, uppkommer också fler hot mot Internets stabilitet och dess användares säkerhet.

Under senare år har problemen med de s.k. botnäten växt globalt. Det finns nu enskilda botnät som består av tiotusentals datorer runt om i världen och kontrollen över botnäten har kommit att bli en viktig handelsvara i den undre världen.

Det har dock varit svårt att avgöra hur situationen ser ut i Sverige. Med tanke på landets höga datoranvändning och bredbandspenetration finns farhågor om att Sverige skulle kunna utgöra en särskilt lämplig grogrund för botnätens tillväxt. I denna rapport redovisar PTS resultatet av en utredning som genomförts, i syfte att söka större kunskap om hur spridningen av botnät ser ut i Sverige och hur marknadens aktörer agerar med anledning av säkerhetshotet.

Marianne Treschow
Generaldirektör

Innehåll

Sammanfattning

Botnät är nätverk bestående av datorer som infekterats med illasinnad kod, som ger personerna bakom botnäten full kontroll över datorerna. Ett botnät kan t.ex. användas till att skicka stora mängder skräppost eller för att utföra överbelastningsattacker. Ofta påverkas inte de användare vars datorer infekterats, vilket gör botnäten säregna bland Internetrelaterade säkerhetshot.

Utbredningen av botnät framhålls ofta som ett av de större hoten mot säkerheten på Internet. Uppgifter talar om flera miljoner drabbade datorer världen över. Flera stora säkerhetsföretag har redovisat uppgifter om botnätens utbredning på en global nivå men det saknas uppgifter om situationen i enskilda länder. Syftet med denna rapport har varit att fastställa botnätens utbredning i Sverige och redovisa denna. Vidare har syftet varit att analysera vilka åtgärder marknadens aktörer vidtar för att komma till rätta med problemet.

Flertalet aktörer saknar dock relevant statistik eller har inte haft möjlighet att bryta ned den på nationell nivå. Eftersom det i stort sett inte är någon Internetleverantör som bevakar utbredningen består de uppgifter som har funnits att tillgå till stor del av uppskattningar. PTS uppskattning är dock att färre än en procent av Sveriges bredbandsanslutna datorer är drabbade.

Flertalet Internetleverantörer arbetar förebyggande för att hjälpa sina kunder att undvika att bli drabbade av säkerhetsproblem. När det gäller kunder som redan drabbats är det dock inte alla som agerar för att komma till rätta med problemet. Vissa aktörer ser av olika skäl hinder mot att vidta långtgående åtgärder. PTS anser att den tekniska utvecklingen bör medföra en utveckling även vad gäller ansvarsfrågor. Även om ingen enskild aktör bär hela ansvaret för att hindra problemen med botnät, är det viktigt att de som har bäst förutsättningar att stävja problemet också vidtar åtgärder. Internetleverantörer torde ha bäst förutsättningar att övervaka trafik och kontakta drabbade slutanvändare. Användarna själva bär ett stort ansvar men de saknar ofta nödvändiga kunskaper för att på egen hand hantera uppkomna säkerhetsproblem. De behöver därför stöd från såväl Internetleverantörer, säkerhetsföretag och andra mjukvaruleverantörer som myndigheter och organisationer.

PTS kommer att fortsätta arbeta med problemen kring Botnät. Det skulle bl.a. vara värdefullt om gemensamma mätmetoder utvecklades av Internetleverantörerna, så att säkrare statistik om läget kunde erhållas. Vidare finns ett behov av att ytterligare utreda och diskutera ansvar och juridiska förutsättningar för att agera mot säkerhetsrelaterade hot på Internet samt eventuellt behov av förändringar i lagstiftningen. Bl.a. för sådana diskussioner skulle kunna PTS anordna ett forum för berörda aktörer i Sverige.

1 Inledning

1.1 Bakgrund

Problematiken kring botnät framställs ofta som ett av de stora säkerhetshoten på Internet. Botnät utgör såväl ett säkerhetshot genom att de kan utnyttjas för reella attacker mot resurser på Internet men även ett hot mot tilliten eftersom de utgör en allvarlig integritetskränkning av den enskilda slutanvändare vars dator blir infekterad och därmed ofrivilligt blir medlem i ett botnät.

Det finns många och skilda uppfattningar om spridningen av botnät och storleken på dessa. Bedömningar som publiceras redogör vanligen för situationen på global nivå och det är därför svårt att få en överblick av hur situationen ser ut på nationell nivå. Sverige ter sig som ett förhållandevis attraktivt land att etablera botnät i, mot bakgrund av att den stora bredbandspenetrationen innebär att många ”vanliga” användare med Internetanslutningar har en förhållandevis stor bandbredd.

1.2 Syfte

Det främsta syftet med studien har varit att utreda möjligheten att få större kunskap om hur spridningen av botnät ser ut i Sverige, dvs. i vilken utsträckning svenska abonnenters datorer är delar av internationella botnät. I den utsträckning sådana uppgifter har kunnat erhållas, har syftet även varit att göra en sammanställning och analys av utbredningen av botnät i Sverige. Vidare har syftet varit att få en inblick i hur Internetleverantörer ser på problemet med förekomsten av botnät och vilka åtgärder de vidtar i anledning av det. PTS har också haft som ambition att belysa några av de problem som är speciella avseende botnät och då särskilt den ansvarfördelning och de skilda uppfattningar om vilka åtgärder som är rimliga att vidta inom ramen för tillhandahållandet av en Internettjänst.

Syftet har inte varit att markera vad utpekade aktörer gör eller inte gör avseende problematiken och av den anledningen namnges ingen av de aktörer som deltagit i intervjuerna.

1.3 Metod

Vad avser utbredningen av botnät i Sverige finns det ett antal tänkbara metoder för att erhålla denna typ av uppgifter. Den metod som har valts består av informationsinhämtning från öppna källor samt djupintervjuer med ett urval av aktörer, såväl inom PTS tillsynssfär (Internetleverantörer) som anknutna aktörer i form av mjukvaruföretag med säkerhetsinriktning (nedan kallade ”säkerhetsföretagen”).

Projektet har tagit del av resultat från tidigare arbete inom området i Sverige, bl.a. den nulägesbeskrivning som togs fram av ett antal myndigheter i september 2005.[1] Det finns även en uppsjö av allmänt tillgängligt material kring botnät publicerat på Internet. Intresseorganisationer, säkerhetsföretag och akademiska institutioner har gett ämnet stor uppmärksamhet, vilket resulterat i rapporter avseende tekniska aspekter, aktuella och kommande användningsområden för botnät samt statistiskt material avseende utbredning och användning. Eftersom fenomenet i grunden är av global karaktär, utgår dock statistik och annat publicerat material genomgående från ett internationellt perspektiv, snarare än det nationella perspektiv som är målsättningen i detta projekt. I viss utsträckning har dock sådant material kunnat användas i projektet.

PTS har även breda kontaktnät på informella och formella plan, genom vilka relevanta uppgifter har kunnat erhållas. Som utgångspunkt för kartläggningen om utbredningen av botnät i Sverige har projektet valt uppgifter som lämnats av Shadowserver, en ideell organisation som ägnar sig åt att kartlägga utbredningen av botnät över hela världen.[2] För att komplettera uppgifterna från Shadowserver har projektet även samlat in uppgifter från två branscher som bedömdes ha goda möjligheter att bidra med statistik; Internetleverantörer och större mjukvaruföretag som arbetar med säkerhetsprodukter för konsumentmarknaden. Projektet har valt att inte gå på bred front och begära in uppgifter i en enkät riktad till alla relevanta aktörer, utan har fokuserat på intervjuer med fem större Internetleverantörer och tre säkerhetsföretag i Sverige.

Under intervjuerna har även frågor om vilka åtgärder som kan och bör vidtas av olika aktörer för att komma till rätta med botnätsproblematiken och relaterade ansvarsfrågor diskuterats. De intervjuade Internetleverantörerna har en sammanlagd marknadsandel avseende bredbandsanslutningar på mellan 80 och 90 % av privatkunder i Sverige. Intervjuerna har genomförts individuellt med en representant som har en teknisk eller informationssäkerhetsbakgrund och, vad gäller Internetleverantörerna, som har god insyn i företagets tekniska infrastruktur.

[1] Rapporten *Botnets, Nulägesbeskrivning, 2005-09-27,* framtagen av Krisberedskapsmyndigheten, Försvarets Radioanstalt, Rikskriminalpolisen/SÄPO, Post- och telestyrelsen, Försvarsmakten och Totalförsvarets forskningsinstitut.
[2] http://www.shadowserver.org

2 Vad är botnät, hur påverkas vi av dem och hur kan de bekämpas?

2.1 Vad är botnät?

2.1.1 En bot låter den infiltrerade datorn fjärrstyras

Ordet bot är egentligen en förkortning av robot. En bot kan beskrivas som ett datorprogram som kan utföra mer eller mindre automatiserade uppgifter. Det finns flera olika typer av botar. En bot kan antingen vara förprogrammerad att utföra vissa enkla uppdrag enligt ett givet mönster, eller ha programmerats att reagera på förändringar i sin omgivning.

Man kan skilja mellan godartade botar och elakartade botar som har skapats för att användas i kriminella eller andra otillbörliga syften. Ett typiskt användningsområde för godartade botar är att samla in information från webbsidor på ett effektivt sätt, en teknik som är vanlig hos sökmotorer. När det talas om botar och botnät idag menar man vanligen elakartade botar och denna rapport berör endast elakartade botar och botnät.

Varje sådan bot lever, likt en parasit, i form av illasinnad kod som installerats i en Internetansluten dator. Den som kontrollerar boten kan sedan fjärrstyra och utnyttja den infiltrerade datorns resurser ofta helt utan datorägarens vetskap. En dator som infekterats med en bot kallas ibland för ”zombie” eller ”drone”. I den här rapporten används dock genomgående ”den infekterade datorn”.

2.1.2 En bot sprids som illasinnad kod över Internet

Botar sprids och verkar i stor utsträckning med användning av kommunikationsvägar som i sig är fullt legitima. Som exempel på vanliga sätt att distribuera botar och annan illasinnad kod kan nämnas bifogade filer till e-postmeddelanden och länkar till webbsidor som har preparerats med illasinnad kod i syfte att infektera besökaren. Det förekommer också att illasinnad kod tillhandahålls integrerat med annan till synes legitim programvara i form av en trojan.

I ovanstående fall krävs att en användare förleds att själv agera på något sätt för att bli infekterad. I andra fall kan dock den illasinnade koden infektera en användare utan någon aktivitet från denne. Detta kan till exempel ske genom utnyttjande av sårbarheter i operativsystemet eller en applikation som används. Redan infekterade datorer kan ha funktionalitet för att systematiskt söka efter andra sårbara datorer på Internet och sprida infektionen vidare. En användare kan på så vis bli infekterad av en bot enbart genom att ansluta sin sårbara dator till Internet.

2.1.3 Botnät styrs centralt av herdar

Genom att botarna är sammanlänkade och direkt eller indirekt kan interagera med varandra och utföra distribuerade uppgifter bildas det nätverk som vanligen kallas för botnät (eng. *botnet*).

Ett botnät kan bestå av allt från ett fåtal till tusentals infekterade och sammanlänkade datorer, spridda över hela världen. Inbyggt i botnäten finns därför en infrastruktur för ledning (eng. *command & control*) som möjliggör för herdar (eng. *herder*) att styra botnätet. Botnäten skiljer sig åt i hur de är uppbyggda och vilka tekniker som nyttjas för att herdarna ska kunna kommunicera med sina botar. Vanligt förekommande kommunikationskanaler är över protokoll som HTTP, P2P eller IRC.[3] Herdarna behöver inte direkt kommunicera med varje bot i nätverket för att kunna kontrollera det. Däremot måste de kommunicera med infrastrukturen för ledning och för att gardera sig mot upptäckt brukar herdarna använda sig av anonymiseringsverktyg som försvårar spårning.

2.1.4 Botnät har flera användningsområden

Botnät har ett flertal möjliga användningsområden och ofta används ett och samma botnät också på flera olika sätt. Ett botnät med flera tusen infekterade datorer kan till exempel användas för att samtidigt anropa en server på Internet. Om servern inte är dimensionerad för att hantera så många användare kan den bli överbelastad och inte längre nås av andra användare (en s.k. distribuerad överbelastningsattack, eng. *distributed denial-of-service attack*). Det är inte ovanligt att denna möjlighet nyttjas för att utöva utpressning mot företag och organisationer. Ett företag vars verksamhet i hög grad är beroende av fungerande elektroniska kommunikationer kan efter hot om en överbelastningsattack se sig tvingat att betala förövarna, för att undgå risken för angrepp. Det finns även exempel på överlastningsattacker som använts i politiska syften, för att t.ex. utöva påtryckningar mot en stat eller organisation. Denna typ av utpressning för ekonomisk eller politisk vinning utgör sannolikt ofta en del av den organiserade brottslighetens verksamhet.[4]

Andra exempel på användningsområden för botnät är stöld av känslig information från användarna av de infekterade datorerna samt för distribution av skräppost. Botarna är ofta konstruerade så att deras användningsområde kan

[3] Med HTTP avses *Hyper Text Transfer Protocol* vilket är det protokoll som normalt används för överföring av webbsidor. P2P står för *Peer to Peer* och är en modell för sammankoppling av noder som inte utgår från att det finns en gemensam server som samtliga noder kommunicerar med (att jämföra med en traditionell klient-server-modell). IRC (*Internet Relay Chat*) är ett system som ursprungligen utvecklades för chatt och diskussioner i forum som kallas för kanaler. I denna ursprungliga tillämpning, används en särskild klientprogramvara som kommunicerar med IRC-servern.

[4] Se t.ex. beskrivningar i *Symantec Report on the Underground Economy, July-07 – June-08*, s. 8-15.

förändras och utvecklas över tiden. När en bot väl installerats i en dator kan den på kommando anpassas till att exekvera i stort sett vilken kod som helst i datorn.

2.2 Hur påverkas vi av botnät?

I detta avsnitt redogörs för hur problembilden ser ut för användarna på Internet och några marknadsaktörer.

2.2.1 Datoranvändare är både mål och medel för botnäten

I någon utsträckning berörs sannolikt varje användare som är uppkopplad mot Internet av problematiken med botnät, antingen som ofrivillig värd för en bot eller som mål för ett botnäts aktiviteter. Flertalet användare torde dock inte utsättas för någon allvarligare påverkan annat än att t.ex. regelbundet få en mängd skräppost, vilket för många inte torde innebära annat än ett irritationsmoment.

Användare vars dator inhyser en bot

För att ett botnät ska kunna växa och nå en storlek som gör att dess aktiviteter får önskad effekt, är det viktigt att den användare vars dator drabbats av en bot inte märker att så har skett och därför inte heller vidtar åtgärder för att rensa datorn från den illasinnade koden. Det förekommer dock att användaren direkt påverkas, t.ex. i samband med att ett botnät används för att utföra överbelastningsattacker, vilket kan leda till att boten tillfälligt nyttjar en stor del av användarens bandbredd mot Internet. Användaren påverkas också om boten har funktionalitet för att stjäla information, till exempel inloggningsuppgifter, från användaren. I de fall där botar används för informationsstöld kan användarna drabbas av stora skador av både ekonomisk och integritetsmässig karaktär.

De negativa effekterna för användaren torde alltså ofta vara indirekta. Denne kan vara tvungen att lägga ned arbete och eventuellt även pengar på att rensa sin dator och i förlängningen löper användaren en risk att få sin Internetanslutning avstängd eller begränsad, se avsnitt 2.3.3.[5]

Användare som utsätts för botnätsaktivitet

En av de vanligaste aktiviteterna riktade mot andra användare än de vars datorer är värdar för botar torde vara massutskick av skräppost. Det är sannolikt en väsentlig del av den mycket stora mängd skräppost som når i stort sett alla användare av e-post, som distribueras med hjälp av botnät. Privatpersoner torde i regel kunna hantera problemet utan att drabbas av

[5] Se vidare PTS rapport *Spionprogram och andra närliggande företeelser*, PTS-ER-2005:15.

någon påtaglig skada, medan företag vanligen tvingas investera i system för e-postfiltrering för att minimera fenomenets påverkan på verksamheten.[6]

Mål för den troligen mest omtalade användningen av botnät, överbelastningsattacker, är vanligen företag och organisationer. Genomförda attacker kan resultera i att det drabbade företaget förlorar intäkter genom att det inte kan kommunicera med sina kunder eller genom att det tvingas betala för att undgå hot om attacker.

2.2.2 Internetleverantörer påverkas främst indirekt

Internetleverantörer kan givetvis drabbas av botnätsaktivitet i egenskap av användare. Vidare hanterar Internetleverantörerna många system, som utgör delar av Internets infrastruktur och är viktiga för Internets grundläggande funktion. Sådana system kan potentiellt vara sårbara för t.ex. överbelastningsattacker och skulle således också kunna utgöra attraktiva mål.

Det kan dock ifrågasättas i vilket utsträckning Internetleverantörerna påverkas i sin egenskap av leverantörer av kapacitet på Internet. Enligt de Internetleverantörer som PTS har intervjuat, utgör botnättrafik endast en mycket liten del av all trafik på Internet. I det fall en överbelastningsattack iscensätts med användning av ett stort antal botar som befinner sig i en viss Internetleverantörs nät torde en märkbar effekt kunna uppstå men sannolikt inte av en dignitet som i någon större utsträckning hotar att stjäla kapacitet från legitim trafik. Vid en dylik attack torde dock den Internetleverantör som tillhandahåller kapacitet till det företag eller organisation som är det direkta målet för attacken kunna påverkas i större utsträckning, då all överbelastningstrafik kanaliseras till dennes nät.

Bortsett från eventuella problem med belastning av tillgänglig kapacitet är dock stor trafikvolym generellt sett positiv för en Internetleverantör, eftersom detta försätter leverantören i en god position vid förhandling av transitavtal. Om en allt för stor del av den trafiken som kommer från en Internetleverantörs nät utgörs av oönskad trafik, såsom skräppost eller annan botnätsgenererad trafik, kan dock motsatt effekt uppnås. Enligt uppgifter från Internetleverantörerna finns det en risk att en sådan leverantör blir känd som källa till oönskad trafik, vilket kan försätta denne i en sämre förhandlingsposition eller försvåra för leverantören att hitta andra Internetleverantörer som är villiga att ingå avtal om peering.

Indirekt löper således Internetleverantörer en viss skaderisk till följd av utbredning av botnät inom deras egna nät, liksom viss skaderisk till följd av

[6] Flertalet Internetleverantörer tillämpar regelmässigt filtrering av misstänkt skräppost för privatkunder.

attacker riktade mot användare, i det egna nätet. Sammantaget uppger dock Internetleverantörerna att de endast i mycket liten utsträckning påverkas av problematiken.

2.2.3 Brister i mjukvara kan utnyttjas

Som tidigare har redovisats, utgör sårbarheter och bristande säkerhetsfunktioner i mjukvara en bidragande orsak till att utbredning av botnät kan ske.[7] De som utvecklar och distribuerar sådan mjukvara torde dock sällan vara direkt drabbade av detta.[8] Den skada de riskerar att drabbas av torde vanligen hänföras till utvecklarens renommé. I samband med publik rapportering om säkerhetsrelaterade problem är det inte ovanligt att brister i operativsystem eller annan vitt distribuerad mjukvara framställs som den främsta orsaken.

2.3 Hur kan botnät bekämpas?

2.3.1 Det finns sätt att upptäcka och spåra botnät

En bot eller ett botnät kan upptäckas och spåras på flera olika sätt. Nedan ges några exempel på vanligt förekommande metoder.

Trafikanalys och kartläggning

Genom att placera ut särskilda system för trafikanalys kan den trafik som passerar i ett nätverk analyseras i syfte att försöka identifiera botnätsrelaterad trafik. Trafiken som skickas i nätet kan t.ex. jämföras med signaturer som beskriver sedan tidigare identifierade trafikmönster. Sådana trafikmönster kan t.ex. beskriva avsändar- och mottagaradresser för botnättrafik (såsom adresser tillhörande ledningsnoder i ett botnät). System för trafikanalys kan varna när sådana trafikmönster upptäcks och rapportera vilka IP-adresser som har blivit eller är på väg att bli en del av ett botnät. Det är möjligt att på motsvarande vis även analysera innehållet i trafiken.

Ett annat tillvägagångssätt för att upptäcka och spåra ett botnät är att under kontrollerade förhållanden fånga in och analysera en bot och dess beteende, till exempel genom att använda en så kallad honungsfälla (eng. *honeypot*). En honungsfälla är ett datasystem med till synes mycket låg säkerhet som kan användas för att locka till sig angrepp och för att till exempel fånga upp illasinnad kod för vidare analys. En bot som fångats upp med hjälp av en hongungsfälla kan analyseras och genom att till exempel låta den infektera en dator under kontrollerade former kan information erhållas om hur den beter sig (vilka anslutningar som görs och på vilket sätt). Vidare kan det vara möjligt

[7] Se avsnitt 2.1.2.

[8] Det är tänkbart att mjukvaruföretag skulle kunna hållas juridiskt ansvariga för skador som orsakats av brister i mjukvaran. Generellt torde dock ett sådant ansvar ha eliminerats genom friskrivningar i avtal.

att låta en egen, specialkonstruerad, bot ansluta sig till och infiltrera ett botnät. Den specialkonstruerade boten kan lyssna på kommandon från herdarna och på så vis samla information om vad botnätet kommenderas att utföra och eventuellt identifiera och lokalisera andra botar i botnätet. Informationen som erhålls om en bot eller ett botnäts beteende kan t.ex. användas för att skapa de signaturer som används vid trafikanalys i syfte att upptäcka botar.

Honungsfällor kan således utgöra ett viktigt led i kartläggningen av ett botnät. För att öka möjligheterna att fånga upp botar på detta vis kan flera honungsfällor, placerade på olika ställen på Internet, kopplas samman i ett s.k. honungsnät (eng. *honeynet*).

Informationsutbyte m.m.

Precis som Internet är ett globalt nätverk, sprids och verkar även botnät globalt. I ett botnät kan ledningsnoden finnas i ett visst land medan såväl botar som målen för botnätets attacker finns utspridda i ett flertal länder över hela världen. Av den anledningen är utbyte av information mellan olika aktörer på Internet en nödvändighet för att åtgärder med mål att hindra ett botnäts spridning eller verkan ska kunna sättas in i tid.

Informationsutbyte kan ske på flera sätt. Enligt ett allmänt etablerat system för s.k. abuse-hantering har normalt varje Internetleverantör en kontaktpunkt dit vem som helst kan höra av sig för att rapportera oönskade aktiviteter som härrör från Internetleverantörens egna nät.

Det finns även företag och organisationer som ägnar sig åt systematisk insamling av information om aktuella säkerhetsproblem, incidenter och pågående attacker. Informationen sprids till relevanta Internetleverantörer, säkerhetsföretag, mjukvaruleverantörer och andra aktörer, t.ex. *Computer Emergency Response Teams* (CERT), som berörs. Vid sidan om denna typ av informationsspridning, finns även många informella nätverk mellan de olika aktörerna, vars syfte är att snabbt kunna utväxla information om pågående attacker eller potentiella hot.

2.3.2 Förebyggande arbete kan begränsa spridningen

Oavsett vilken metod som används för distribution av den illasinnade koden genom vilken ett botnät kan växa, finns det i varierande utsträckning metoder som kan begränsa att botnätet sprids, att botar kan kommunicera med herdarna eller att botar kan utföra de uppdrag som beordras.

Råd och dåd för att öka användares medvetenhet och möjlighet att skydda sig

Som konstaterats ovan kan botnät växa genom att illasinnad kod sprids, huvudsakligen genom att användare förleds att själva installera den eller genom att sårbarheter i operativsystem och annan programvara utnyttjas. Såväl myndigheter som Internetleverantörer, säkerhetsföretag, mjukvaruleverantörer och andra organisationer kan bidra till att minska risken för spridning av illasinnad kod genom informationsinsatser som ökar användarnas medvetenhet om riskerna och deras kunskap om hur de kan skydda sig.

Det är t.ex. högst sannolikt att botnätens möjligheter att växa skulle begränsas betydligt, om en högre andel av användarna hade brandvägg och antivirusprogram installerade samt regelbundet uppdaterade sådana säkerhetsprogram, operativsystem, webbläsare och annan programvara.

Likaså torde risken för att infekteras av en bot vara avsevärt lägre bland de användare som lärt sig att undvika skräppost och att vara mycket försiktiga med att öppna bifogade filer eller klicka på länkar i e-postmeddelanden.

Blockering av trafik för att förhindra botnät från att verka

Enligt en etablerad metod är det möjligt för Internetleverantörerna att blockera vissa portar i syfte att minska att deras nät används för otillbörlig trafik.

Som exempel är det möjligt för Internetleverantörer att minska risken för att deras kunders Internetanslutningar används för att skicka skräppost genom att blockera port 25 (som normalt används av SMTP-protokollet för att skicka e-postmeddelanden). Användarna måste då använda Internetleverantörens e-postservrar för att skicka meddelanden. Internetleverantörens e-postservrar kan konfigureras så att autentisering krävs eller andra villkor uppställs, vilket ger leverantören kontroll över utgående e-post. På detta sätt försvårar man även för botar att distribuera skräppost. Utan en sådan blockering kan en bot som har funktionalitet inbyggt för att distribuera e-post användas för att skicka en stor mängd skräppost. Det förekommer dock botnät som utnyttjar andra kanaler, t.ex. webbaserade e-posttjänster, för att skicka skräppost. När sådana andra kanaler används har det ingen betydelse att port 25 har blockerats. Den stora variationen mellan olika botnät gör det svårt att stoppa trafiken genom den förhållandevis enkla och grovkorniga filtrering som spärrning av enskilda portar åstadkommer.

En mer komplex och anpassningsbar metod bygger på användning av särskilda system som genom trafikanalys försöker identifiera skadlig trafik och blockera denna innan den når mottagaren. Denna typ av blockering nyttjas t.ex. i s.k. *Intrusion Prevention Systems*.

2.3.3 Tillväxt och skador kan begränsas

Det kan finnas möjligheter att begränsa ett botnäts tillväxt eller till och med oskadliggöra botnätet genom att stänga ned dess infrastruktur för ledning. Dessa möjligheter varierar dock mellan olika botnät, bl.a. beroende på hur infrastrukturen för ledning är uppbyggd. I detta avsnitt redovisas några generella metoder som kan vara effektiva för att förhindra botnätens tillväxt eller skadeverkningar.

Det kan finnas möjligheter att stoppa pågående tillväxt av ett botnät eller pågående botnätsaktivitet såsom överbelastningsattacker inom det egna området. Det är normalt endast Internetleverantörer som har sådana möjligheter, då det främst handlar om att strypa eller i vart fall kraftigt begränsa möjligheten till kommunikation till eller från vissa IP-adresser.

En åtgärd som dock inte är av tekniskt komplicerad karaktär är att söka kontakt med användare som upptäckts husera en bot, i syfte att lämna upplysningar och råd så att användaren själv kan lösa problemet. Åtgärden ger sannolikt inte tillräckligt snabbt resultat för att kunna förhindra pågående botnätsaktivitet som kommer från användarens dator. Upptäcks emellertid botar innan de hunnit tas i bruk i något illasinnat syfte, kan åtgärden bidra till at begränsa en nära förestående attack och även verka preventivt genom att bidra till användarens förståelse för och kunskap om problemet.

När eventuella förebyggande åtgärder inte har kunnat förhindra spridningen av ett botnät och en Internetleverantör får kännedom om förekomsten av botar i det egna nätet, kan det finnas tekniska möjligheter att isolera berörda användare i syfte att förhindra möjligheten för botarna att agera. Isolering kan ske genom att Internetanslutningen helt stängs, men även genom att anslutningen begränsas på så vis att endast viss trafik tillåts, t.ex. webbtrafik till säkerhetsföretag och mjukvaruleverantörers uppdateringstjänster. Avsikten med den senare tekniken (på engelska benämnd *walled garden*) är att användaren ska ges möjlighet att åtgärda den drabbade datorn, samtidigt som boten förhindras att verka.

I avsaknad av fungerande förebyggande åtgärder och isolering av användare så finns det normalt ingenting som begränsar ett botnäts möjligheter att initiera t.ex. en överbelastningsattack. Under förutsättning att de uppmärksammar en pågående attack, kan dock ofta Internetleverantörer i vars nät de aktiva botarna finns, vidta tillfälliga åtgärder för att hindra den aktuella botnättrafiken, t.ex. blockering av trafik som går över vissa portar eller som har en viss destination.

3 Hur ser utbredningen i Sverige ut?

3.1 Statistik från intervjuade aktörer

Alla de aktörer PTS har intervjuat har kunnat lämna statistik över upptäckta botar. Siffrorna har tagits fram på olika sätt och med stor variation i metodens precision.

Kortfattat kan sägas att säkerhetsföretagens statistik baseras på användning av honungsnät eller andra slags mätpunkter för att samla data om vilka botnät som är aktiva och deras utbredning. I viss utsträckning används även infiltration av botnät för att närmare kartlägga deras funktion och utbredning.

Internetleverantörernas statistik baseras antingen på abuse-anmälningar och information om upptäckta botar som erhållits genom informationsutbyte i olika informella nätverk eller på information man erhållit genom analys av trafikmönster eller annan automatisk övervakning av det egna nätet.

Genomgående kan sägas att mätningarna inte har skett regelbundet utan mer sporadiskt och i vissa fall endast på PTS förfrågan. Samtliga Internetleverantörer saknar därmed också historisk statistik och har bara kunnat förmedla en uppskattning av hur mängden förändrats över tiden.

Shadowserver är en organisation som har specialiserat sig på att spåra botnät och analysera dess utbredning i världen.[9] Shadowserver har under perioden januari till september 2008 observerat i snitt 1436 unika svenska IP-adresser per månad, som tillhörde något av de botnät som Shadowserver känner till och övervakar.

Uppgifterna överensstämmer väl med de uppgifter som ett av säkerhetsföretagen lämnat, avseende antalet botar i Sverige. Företaget övervakar c:a 60 olika botnät och har under september 2008 registrerat 1 400 unika IP-adresser .

Enligt de mätningar som ett annat säkerhetsföretag gjort upptäcktes totalt 20 090 botar sammantaget under första halvåret 2008.[10] Mot beaktande av att varje bot enligt företaget är aktiv i snitt i tre månader, torde uppgiften motsvara c:a 10 000 aktiva botar per månad. Uppgifterna härrör från ett nätverk av över 40 000 sensorer runt om i världen, vilket skulle kunna förklara varför företaget upptäckt fler botar än de två föregående organisationerna.

[9] Se vidare bilaga 1.
[10] Som jämförelse upptäcktes 14 818 botar under det första halvåret 2007.

Bland de Internetleverantörer som baserade sin statistik på automatiserad mätning, uppger en att man vid mättillfället i slutet av oktober 2008 observerade 5 000 botar i sitt nät, vilket omräknat till det totala antalet bredbandsanslutningar i Sverige motsvarar c:a 27 000 botar. En annan jämnstor Internetleverantör uppger att mellan 100 och 150 botar upptäcks per vecka. Under antagandet att varje bot lever tre månader, motsvarar detta c:a 1500 vid varje tillfälle aktiva botar. Omräknat till den totala populationen av bredbandsanslutningar, blir det totala antalet svenska botar c:a 9 500.

Uppgifterna från de Internetleverantörer som baserar sin statistik på manuellt insamlad information, t.ex. abuseanmälningar, varierar i intervallet 5-10 upp till 25 behandlade ärenden per arbetsdag, uppgifter som inte med lätthet kan jämföras med de per automatik insamlade uppgifterna från övriga aktörer.

Flertalet av de intervjuade aktörerna poängterade att de konkreta siffror som lämnades inte utgör hela sanningen. Generellt befaras att det finns ett betydande mörkertal av botar bland svenska Internetanvändare. Som exempel kan nämnas att det säkerhetsföretag som uppmätt 1 400 botar under en månad, ansåg att en rimlig uppskattning av det totala antalet botar är c:a 10 000 – 15 000. Majoriteten av de intervjuade är dock av uppfattningen att problemet med botnät har minskat något de senaste åren.

Tabell 1 Antal svenska botar, i förhållande till det totala antalet bredbandsabonnemang.

Uppmätt antal aktiva svenska botar, omräknat i förhållande till det totala antalet svenska bredbandsabonnemang. Utgår från genomsnittlig livstid på 3 mån. per bot.

	Uppmätt antal	Omräknat antal	Andel
Shadowserver	1 436 i snitt per månad	1 400	0,04 %
Säkerhetsföretag 1	1 400 under en månad	1 400	0,04 %
Säkerhetsföretag 2	20 090 under ett halvår	10 000	0,29 %
Internetleverantör 1	5 000 vid ett tillfälle i egna nätet	27 000	0,78 %
Internetleverantör 2	100 – 150 per vecka i egna nätet	9 500	0,27 %
Totalt antal abonnemang, juni 2008		*3 475 000*	*100 %*

3.2 Slutsatser av uppgifterna

3.2.1 Stora skillnader föreligger i underlaget från aktörerna

PTS kan konstatera att det föreligger stora skillnader i antalet upptäckta botar. Spannet mellan det minsta och det största antalet är mycket stort. Generellt kan sägas att de uppgifter bland Internetleverantörer som baserades på manuell insamling var lägre än de som togs fram med hjälp av analys av trafikmönster eller annan automatiserad övervakning. De automatiserade övervakningsmetoderna skiljer sig också åt mellan de olika aktörerna och det finns stora skillnader i antalet mätpunkter.

Det uppmätta antalet beror också på hur långa mätperioderna är. Gemensamt för de automatiserade mätningarna är att de registrerar de IP-adresser som används av de upptäckta botarna. Varje dag mätningen pågår upptäcks ett antal nya IP-adresser. Vanligen går det dock inte att avgöra om en ny IP-adress innebär att ännu en dator infekterats eller om det rör sig om en sedan tidigare infekterad (och registrerad) dator som har tilldelats en ny IP-adress. Eftersom flertalet Internetleverantörer använder sig av dynamisk IP-adresstilldelning är det troligt att en och samma dator över tiden kommer att ha tilldelats olika IP-adresser. Ju längre mätningen pågår, desto större torde det antal infekterade datorer vara, som hunnit få nya IP-adresser och därför registrerats mer än en gång.

Härtill kommer att mätningarna endast kan ta hänsyn till nytillkomna infekterade datorer. Det finns inget säkert sätt att avgöra om en bot har eliminerats (t.ex. pga. att användaren rensat datorn med hjälp av antivirusprogramvara). Det faktum att en bot inte varit aktiv sedan en viss tid kan lika gärna bero på att den infekterade datorn inte varit påslagen under denna tid. Generellt medför detta att en uppgift om antalet existerande botar blir högre ju längre tid mätningen pågått.

Vissa uppgifter avser istället antalet aktiva botar vid en vis tidpunkt. För att kunna göra en sådan uppskattning måste dock ett antagande göras om att de botar som uppvisat livstecken under en viss period ska betraktas som aktiva. Med utgångspunkt i uppskattningar av hur ofta datorer används och hur ofta de tilldelas en ny dynamisk IP-adress kan man t.ex. göra antagandet att alla botar (IP-adresser) som har uppvisat livstecken de senaste 10 dagarna ska anses vara aktiva vid en given tidpunkt.

De uppgifter som lämnats till PTS inför denna rapport är baserade på olika mätmetoder, mätperioder och antal mätpunkter. Dessa faktorer torde utgöra de främsta orsakerna till att siffrorna varierar kraftigt mellan de olika uppgiftslämnarna och gör det mycket svårt att jämföra eller sammanställa

statistiken. Det är med stöd av dessa uppgifter inte möjligt att ge en särskilt exakt uppgift om hur stor andel av Internetanslutna datorer i Sverige som är infekterade.

3.2.2 Det är troligen färre än en procent av Sveriges datorer som är drabbade

En grov uppskattning av de uppgifter som givits myndigheten ger vid handen att i vart fall färre än en procent av Sveriges bredbandsanslutna datorer var infekterade under september 2008.

Som jämförelse till uppskattningen kan nämnas att F-secure i sin rapport för andra halvåret 2008 bedömt en nationell spridningsgrad på 1 % vara mycket låg.[11] Detta skulle tala för att spridningsgraden i Sverige i internationell jämförelse är låg. De Internetleverantörer som bedriver verksamhet även i andra länder framförde även uppfattningen att Sverige har en märkbart lägre andel infekterade datorer än andra länder. Det bör dock poängteras att mörkertalet är okänt.

Att Sverige ligger förhållandevis bra till vid en internationell jämförelse kan enligt de intervjuades uppfattning bero på ett antal faktorer.
Sverige har en hög grad av IT-mognad bland sina användare och det finns en relativt sett hög riskmedvetenhet. Det leder till att fler skyddar sig med hjälp av olika säkerhetsmjukvaror. Dessutom jobbar ett antal Internetleverantörer proaktivt genom att erbjuda antivirusprogram till låga priser eller helt gratis till sina kunder. Som framförts av ett av säkerhetsföretagen kan ett annat skäl till Sveriges relativt sett goda position med avseende på botnät vara att andelen piratkopierade operativsystem är färre här än i många andra länder. Utan en licensierad version av ett operativsystem så får man inte alltid tillgång till de säkerhetsuppdateringar som regelbundet publiceras och man är således betydligt mer utsatt för säkerhetsbrister.

Det finns dock även uppgifter som talar emot den statistik som lämnats av de intervjuade aktörerna. PTS har till exempel tagit del av uppgifter från OECD som anger att c:a 4 % av alla botar i världen finns i Sverige. Detta kan jämföras med det faktum att endast c:a 0,6 % av världens Internetanslutna datorer finns i Sverige, något som tyder på att Sverige har en högre andel botar än genomsnittslandet. Enligt samma uppgifter har även andelen attacktrafik som kommer från Sverige ökat till 4 % under tredje kvartalet 2008. Andelen datorer

[11] http://www.f-secure.com/2008/2/index.html

som infekterats med en bot har även ökat med c:a 25-30 % under år 2006-2007.[12]

[12] Uppgifterna härrör från en kommande OECD-rapport, *Communications Outlook 2009*.

4 Hur agerar marknadens aktörer?

4.1 Aktörernas åtgärder mot botnät

4.1.1 Alla aktörer bedriver förebyggande arbete

Som en indirekt skyddsåtgärd mot spridning av illasinnad kod, tillhandahåller flertalet av de Internetleverantörer PTS intervjuat antivirusprogramvara till sina kunder i anslutning till bredbandstjänsten. Vanligen utgör programvaran en tilläggstjänst som ingår utan extra kostnad under en inledande period, för att därefter, med något undantag, betinga en viss månatlig kostnad. Avsikten är att öka användningen av antivirus på kundernas datorer och framförallt att säkerställa att programvaran hålls uppdaterad. Det är sedan flera år tillbaka vanligt att antivirusprogram ingår vid köp av en ny dator, men att uppdateringar endast ingår för en kort initial period. Därefter förväntas kunden teckna ett separat uppdateringsabonnemang, något som ofta inte sker. Lösningen att låta en uppdaterad säkerhetsprogramvara utgöra en slags prenumerationstjänst kopplad till bredbandsabonnemanget, framhålls därför av Internetleverantörerna som ett mer ändamålsenligt alternativ. Ingen av de intervjuade leverantörerna har dock kunna lämna några uppgifter om hur stor andel av kunderna som väljer att prenumerera på säkerhetstjänsten.

Några av Internetleverantörerna tillhandahåller grundläggande information om säkerhetsrisker förknippade med användning av Internet, som syftar till att öka användarnas medvetenhet och kunskap om hur man kan skydda sig. Några av företagen erbjuder mot avgift även privatpersoner hjälp med bl.a. säkerhetsrelaterade problem per telefon. Det har dock inte framkommit att företagen tillhandahåller information eller genomför aktiviteter med specifik inriktning mot botnät.

Säkerhetsföretagen arbetar av naturliga skäl proaktivt med att kontinuerligt eftersöka nya typer av hot eller presumtiva hot. De deltar även i nätverk med andra säkerhetsföretag och mjukvaruleverantörer, som kontinuerligt delar information mellan sig avseende spridningen av botnät och var drabbade datorer kan finnas.

Mjukvaruleverantörer bedriver fortlöpande utveckling för att förbättra sina produkters förmåga att upptäcka och eliminera illasinnad kod. Inom ramen för detta arbete bedrivs även visst utrednings- och forskningsarbete som bl.a. syftar till att kartlägga förekomst och utbredning av de fenomen som hotar säkerheten på Internet som till exempel botnät. Ofta tillhandahåller mjukvaruleverantörer även information till kunder om säkerhetsrisker och

annan verksamhet för att förebygga säkerhetsrelaterade problem, såsom botnät.

I sammanhanget kan nämnas att även PTS arbetar aktivt för att öka allmänhetens medvetenhet och kunskap om Internetsäkerhet. På myndighetens webbplats lämnas information och råd till Internetanvändare och med hjälp av verktyg på särskilda webbplatser kan användare testa säkerhetsnivån på den egna datorn.[13] PTS verkar även aktivt för ett ökat informationsutbyte genom att driva Sveriges nationella CERT, Sveriges IT-incidentcentrum (Sitic).[14] Myndigheten följer löpande utvecklingen inom säkerhetsområdet och kan t.ex. ta fram råd och rekommendationer till branschen eller förslag till lagändring, när så bedöms nödvändigt.

4.1.2 Endast ett fåtal Internetleverantörer söker aktivt efter botnät

Tre Internetleverantörer uppger att de i någon utsträckning genom analys av trafikmönster söker efter misstänkta mönster som kan tyda på att botar i ett botnät kommunicerar med varandra. Ingen av aktörerna har uttryckligen angivit att de utför analys av själva innehållet i kommunikationen. Det är endast en Internetleverantör som i centralt placerade mätpunkter regelbundet analyserar trafik i nätet. Av de som bedriver någon form av trafikanalys är det ingen som uppger att detta sker primärt i syfte att upptäcka botnät eller annan illasinnad aktivitet.

En av Internetleverantörerna uppger att de använder sig av honungsfällor för att upptäcka botar i det egna nätet. Av säkerhetsföretagen uppger ett att man förfogar över ett omfattande globalt nätverk av honungsfällor som bl.a. används för att samla information om sårbarheter i egna mjukvaror.

Ingen av de intervjuade Internetleverantörerna arbetar med att spåra eller kartlägga botnät utanför sina egna nät utan förlitar sig i det avseendet på sådan information som inhämtas genom utbyte med andra aktörer.

Samtliga Internetleverantörer som intervjuats uppger att de tar emot abuse-anmälningar. Två uppger dock att de i princip inte kan beakta denna typ av anmälningar, då volymen av meddelanden är alltför stor och anmälningarnas dignitet är svår att värdera.

Säkerhetsföretagen deltar i stor utsträckning i olika former av internationella samarbeten och arbetar aktivt med att inhämta och sprida säkerhetsrelaterad information. Deltagandet i denna typ av informationsutbyte varierar dock

[13] Se https://www.testadatorn.se/ respektive https://www.testalosenord.se/.
[14] Se http://www.sitic.se/.

bland Internetleverantörerna. Ett par uppger att man i princip endast agerar på information som lämnas av brottsbekämpande myndigheter. Endast en Internetleverantör uppger att man även är aktiv globalt i olika organ som arbetar med säkerhetsfrågor. Två av Internetleverantörerna driver dock en egen CERT-verksamhet.

4.1.3 Ingen Internetleverantör blockerar botnättrafik

Baserat på vad som framkommit vid PTS intervjuer och tidigare undersökningar som myndigheten har genomfört, tillämpar i stort sett samtliga Internetleverantörer som tillhandahåller Internetuppkoppling åt privatkunder portblockering avseende utgående e-post (port 25).

Det är dock ingen av de Internetleverantörer som PTS har intervjuat som uppger att de utför någon form av blockering baserad på trafikanalys i sitt nät, vare sig på central- eller accessnätsnivå.

Undantaget är en specifik form av trafikblockering som flertalet Internetleverantörer tillämpar, för att förhindra leverans av skräppost som skickas till kunder i leverantörens nät. Genom att analysera såväl trafikdata (t.ex. avsändarens e-postadress eller IP-adress) som innehållet i enskilda e-postmeddelanden görs en automatiserad sannolikhetsbedömning av huruvida meddelandet utgör skräppost eller inte. Meddelanden som klassificerats som skräppost raderas antingen omgående eller sorteras till en särskild e-postmapp, för att mottagaren ska få möjlighet att göra en egen bedömning. Någon Internetleverantör tillhandahåller denna typ av filtrering av inkommande e-postmeddelanden som en valbar tjänst, medan flertalet tillämpar obligatorisk filtrering av all inkommande e-post. Sådan blockering av inkommande skräppost har förvisso inte någon direkt relevans avseende botnät, men det är ett intressant faktum att denna typ av blockering är utbredd och väl använd medan blockering av mer renodlad botnättrafik eller annan illvillig trafik är mindre utbredd.

4.1.4 Alla Internetleverantörer agerar inte när botar upptäcks

När väl en eller flera botar upptäckts bland leverantörens kunder skiljer sig aktörerna beteende åt.

Internetleverantörerna tillämpar olika principer för i vilka situationer en användare kontaktas med anledning av att användarens dator deltar i ett botnät eller på något annat sätt utnyttjas för oönskade aktiviteter.

Nära hälften av de intervjuade leverantörerna uppger att man inte vidtar någon åtgärd enbart på grundval av information om förekomsten av en bot; för att

agera krävs i normalfallet en polisanmälan eller att Internetleverantörens egna nät hotas, t.ex. genom överbelastning eller intrång i Internetleverantörens egna system. Den åtgärd som då normalt vidtas är omedelbar avstängning av den berörda anslutningen. Kontakt med användaren sker då först i efterhand.

Övriga Internetleverantörer som har privatkunder uppger dock att man regelmässigt kontaktar drabbade användare per telefon, e-post eller vanlig post så snart man får kännedom om att användaren drabbats av ett problem som kräver åtgärd och uppmanar denne att genomsöka sitt system med ett antivirusprogram. Två av leverantörerna erbjuder även Internetbaserade verktyg för genomsökning av sin dator efter illvillig kod som kunderna kan nyttja.

Först efter upprepade kontaktförsök vidtas någon annan åtgärd, såsom avstängning eller begränsning av anslutningen. Av Internetleverantörerna uppger hälften att det kan förekomma att användares anslutningar helt stängs på grund av att användarens dator deltar i ett botnät. Det sker dock endast om användaren inte hörsammat uppmaningar att rensa sin dator. En av Internetleverantörerna tillämpar ett system med begränsad tillgång till Internet istället för total blockering av anslutningen.[15]

4.2 Hinder mot att vidta åtgärder

Som konstaterats ovan finns det skillnader i Internetleverantörernas förhållningssätt till förekomsten av botar i det egna nätet. Av de tillfrågade Internetleverantörernas svar kan i huvudsak två skäl till att underlåta att vidta ytterligare åtgärder utkristalliseras, ekonomiska och legala skäl.

4.2.1 Ekonomiska och konkurrensmässiga skäl kan hindra

Flera av Internetleverantörerna har påpekat att det saknas ekonomiska incitament att satsa på aktiva åtgärder för att komma till rätta med botnätsproblematiken i det egna nätet.

Med undantag för de allra minsta leverantörerna löper inte Internetleverantörer någon påtaglig risk för att drabbas av oförmånliga transitavtal eller andra negativa konsekvenser i sina relationer med andra leverantörer. Eftersom merparten av användarna inte upplever botnät som ett stort problem i dagsläget, ställs det heller inte i någon större utsträckning krav från kunder på

[15] Se avsnitt 2.3.3.

att leverantörerna ska vidta åtgärder mot botnät.[16] Flertalet Internetleverantörer upplever därför inte heller att en satsning på sådana åtgärder kan motiveras av konkurrensmässiga skäl.

Det har snarare framkommit att en Internetleverantör som vidtar långtgående åtgärder mot botnät kan drabbas av andra, indirekta kostnader och nackdelar ur konkurrensperspektiv.Tekniska spärrar eller begränsningar, som införs i syfte att förhindra trafik som kan relateras till botnät eller annan oönskad aktivitet, medför ofta en viss risk för att även legitim trafik förhindras. Ett välkänt exempel på detta är att de flesta filter mot skräppost ibland fångar för mottagaren välkomna e-postmeddelanden. En risk för den Internetleverantör som tillhandahåller en sådan blockering, är att användarna uppfattar begränsningen som störande i deras legitima användning av Internetanslutningen och att den tjänst som leverantören tillhandahåller därmed kommer att betraktas som sämre än motsvarande tjänst, utan liknande begränsningar, som tillhandahålls av en konkurrent.

I sammanhanget kan dock påpekas att de Internetleverantörer som aktivt kontaktar användare vars datorer har kommit att bli del i ett botnät, uppger att kunderna vanligen uppskattar leverantörens initiativ och i vissa fall även har efterfrågat Internettjänster som är begränsade på så vis att endast de vanligaste användningsfallen, såsom webbsurfning och e-post, är tillgängliga.[17]

4.2.2 Osäkerhet råder om de rättsliga förutsättningarna för åtgärder

Vid sidan av de ekonomiska och konkurrensmässiga orsakerna, har flera Internetleverantörer påpekat att det råder osäkerhet om i vilken utsträckning det är tillåtet för en leverantör att aktivt övervaka nätet för att spåra och eventuellt blockera trafik som kan anses oönskad, t.ex. trafik innehållande illasinnad kod eller trafik som genereras av en bot.

Som redogjorts för ovan, innebär sådan övervakning att Internetleverantören med automatiska medel inspekterar trafiken som överförs i nätet och på olika sätt analyserar den för att avgöra om trafiken är legitim eller inte. Emedan sådan trafikanalys i regel accepteras inom privata nätverk, såsom inom ett företag eller organisation, har Internetleverantörerna framfört att det råder

[16] Enligt PTS individundersökning 2008 upplever användarna främst problem med skräppost (38 %), virus (24 %) och/eller spionprogramvara (18 %). Med reservation för att det inte alltid är lätt för en användare att klassificera de problem han eller hon upplever, är det endast 4 % som uppger sig ha upplevt problem med någon annan typ av intrång på datorn. Se vidare http://www.pts.se/upload/Rapporter/Tele/2008/2008-24-individundersokning-2008.pdf.

[17] Jfr. avsnitt 2.3.3 angående användningen av en sådan begränsad tillgång till Internet, som ett medel mot ett botnäts spridning.

osäkerhet kring i vilken utsträckning det finns acceptans för detta avseende allmänt tillgängliga nät.

Orsaken till denna osäkerhet torde främst vara att utgångspunkten i svensk lagstiftning är att innehållet i elektroniska meddelanden och trafikuppgifter som hör till dessa endast får behandlas av berörda användare. Som konstaterats ovan kan trafikanalys i syfte att spåra botnättrafik avse såväl trafikuppgifter som innehåll i enskilda datapaket.[18]

4.2.3 Det finns farhågor om ändamålsglidning

Några Internetleverantörer har även uttryckt farhågor om att en analys av trafiken utifrån säkerhetsrelaterade principer kan leda till att krav från t.ex. brottsbekämpande myndigheter ställs på Internetleverantören att utföra analyser och blockering av annan typ av kommunikation som av olika anledningar anses som mindre lämplig, såsom t.ex. fildelning av upphovsrättsskyddat material. Även denna potentiella utveckling har därför angivits som skäl mot att införa säkerhetsrelaterad trafikanalys.

4.3 Aktörernas syn på den egna rollen

Vilket arbete som bedrivs och vilka åtgärder som vidtas av respektive aktör skiljer sig givetvis beroende av vilken kategori aktören tillhör; en Internetleverantör agerar under andra förutsättningar än ett säkerhetsföretag eller en mjukvaruleverantör.

4.3.1 Alla Internetleverantörer uppfattar inte sin roll på samma sätt

Vid samtal med leverantörer av Internettjänster uppträder en delvis splittrad syn. Samtliga aktörer har i intervjuer uppgett att de ser botnät som ett problem, både av den anledningen att kunderna som är en del av ett botnät är drabbade av illasinnad kod, men också eftersom deras kunder kan drabbas av följderna av botnät. Internetleverantörerna är dock genomgående av uppfattningen att botnät i dagsläget inte på allvar kan hota driftsäkerheten i deras nät. Man anser sig ha god kontroll över utvecklingen.

Samtliga av Internetleverantörerna uppfattar att deras roll i första hand är att se som tillhandahållare av kommunikationstrafik. De ser således sin roll primärt som att de ska vidarebefordra den kommunikation som skickas utan att värdera eller analysera den. Vissa av leverantörerna ser dock även att deras roll innefattar ett ansvartagande för sina kunder och vill erbjuda dessa ett skydd mot botnät. Ett sådant skydd kan vara att de tillhandahåller säkerhetspaket i

[18] Förbudet mot avlyssning stadgas i 6 kap. 17 § lagen (2003:389) om elektronisk kommunikation. Med trafikuppgift avses enligt 6 kap. 1 § ”uppgift som behandlas i syfte att befordra ett elektroniskt meddelande via ett elektroniskt kommunikationsnät eller för att fakturera detta meddelande”.

form av antivirusprogram och/eller brandväggar som en del av Internettjänsten.

När det gäller hanteringen av kunder som konstaterats vara en del av ett botnät framträder dock en splittrad bild av aktörernas syn. Även om samtliga uppger att de anser botnät utgöra ett problem både utifrån perspektivet att deras kunder kan vara drabbade såsom ofrivilliga medlemmar av ett botnät och såsom presumtiva mål från en attack som sker från ett botnät har de dock olika uppfattningar om sin egen roll gentemot sina kunder.

Medan vissa Internetleverantörer anser att det ligger i deras roll att reagera och ta ansvar för de egna kunderna, har vissa direkt angivit att den traditionella rollen som en Internetleverantör har är att enbart leverera den trafik som skickas, inte att värdera huruvida den trafiken är bra eller dålig och agera därefter. I linje med den synen är också att kunden själv får ta ansvar för den trafik de skickar och det säkerhetsskydd kunden upplever vara nödvändigt för att skydda sig. Om man ska se bortom den principiella uppfattningen om leverantörens egen roll så återkommer bland de leverantörer som inte vidtar några åtgärder även uppfattningen att en kontakt med kunden avseende problemet kommer att leda till merkostnader för företaget, eftersom en kundkontakt med största sannolikhet leder till att kunden återkommer till leverantören och efterfrågar vad kunden de facto ska göra för att lösa problemet. Kundkontakter orsakar alltid en kostnad i form av arbetstid för leverantörens supportpersonal. Denna presumtiva kostnad kombinerat med att ingen direkt vinning upplevs finnas i hanteringen för leverantörens egen del leder till att incitamentet att kontakta kunder inte är stort. En av leverantörerna har angivit kostnadsaspekten som en primär anledning till att inte kontakta kunder avseende denna typ av problem.

De operatörer som kontaktar sina kunder har uppgivit att de anser att hanteringen är rimlig och att det ligger i deras intresse att se till att deras kunder inte drabbas i onödan men även ett sätt att säkerställa att deras kundkrets inte innefattar några växande mängder av botnät, således att ”hålla rent” i det egna nätet. Dessa leverantörer upplever att kunder mycket sällan är negativt inställda till kontakten utan tvärtom att de flesta är tacksamma för påpekandet.

4.3.2 Säkerhetsföretagens roll är tydlig

Vid samtal med säkerhetsföretag ser de av naturliga skäl botnäten som en naturlig del av det hot de arbetar med att bekämpa. Säkerhetsföretagen ser som sitt primära uppdrag att tillhandahålla produkter som antingen hindrar kunder från att bli drabbade av illasinnad kod eller i vart fall som i efterhand kan ta

bort den kod som installerats och rensa kundens dator från botar eller annan illasinnad kod.

5 Vem bär ansvaret för att agera och vilka åtgärder bör vidtas?

Ett mål med denna rapport är att belysa några av de problem som är speciella avseende botnät och då särskilt den ansvarfördelning och de skilda uppfattningar om vilka åtgärder som är rimliga att vidta inom ramen för tillhandahållandet av en Internettjänst. Myndigheten har dock inte någon ambition att inom ramen för denna rapport lämna några färdiga lagförslag eller utpeka en ansvarig aktör som skulle anses ha några särskilda skyldigheter att vidta åtgärder. Den information som finns att tillgå ger inte heller några indikationer på att antalet slutanvändare som är drabbade på så vis att deras datorer infekterats med en bot och blivit del i ett botnät skulle vara så alarmerande att några sådana förslag ens vore rimliga. Det är dock ställt bortom allt tvivel att problematiken finns och knappast kommer att försvinna inom överskådlig tid. Som PTS angivit i rapporten *Strategi för ett säkrare Internet i Sverige* [19], är ett av de stora problemen på Internet idag den bristande säkerheten i de enskilda Internetanvändarnas miljöer. Detta innebär inte bara en risk för den enskilda användarens integritet eller egendom utan även för Internets funktion i stort. Botnät gör denna problematik särskilt tydlig.

Samtliga parter, såväl Internetleverantörer som säkerhetsföretag, som PTS intervjuat har sagt att de ser allvarligt på problematiken. PTS ser det som viktigt för frågans fortsatta diskussion att inte endast frågans allvar eller att botnätens utbredning diskuteras utan också vilket ansvar som kan tas av aktörerna i frågan och vilka åtgärder som är rimliga, effektiva och meningsfulla utifrån detta ansvar.

5.1 Ansvaret för att agera mot botnäten

5.1.1 Ingen aktör bär ensam ansvaret

Det är naturligtvis lätt att påpeka att den som ytterst har ansvar för spridningen och nyttjandet av botnät är den förövare som de facto utvecklat bot-mjukvaran, sett till att den spridits och nyttjar dess kapacitet för illvilliga aktiviteter. Denna rapports fokus är dock inte den snarast polisiära uppgiften att tillse att dessa aktörer på något sätt ställs till ansvar för sitt agerande, eller att redovisa eventuella problematiska juridiska frågeställningar kring frågan om vilka delar av aktiviteterna som faller under ren brottslagstiftning och vilka som inte gör det. Denna rapports fokus är snarare att titta på de aktörer såsom leverantörer av kommunikationstjänster och deras kunder och i vilken

[19] PTS-ER-2006:12. Se http://www.pts.se/upload/Documents/SE/strategi_sakrare_internet_2006_12.pdf.

utsträckning man kan säga att ansvaret fördelas, eller ens finns inom denna grupp.

Botnät utgör ett problemområde som ställer särskilda krav på bedömningen av vilka roller som olika aktörer har. Problemet är delvis ett säkerhetsproblem kring innehållsrelaterade frågor. Den illasinnade kod som installerar botar på slutanvändares datorer sprids på motsvarande sätt som t.ex. maskar och virus, vilket har beskrivits närmare i avsnitt 2.1.2.

Vad gäller denna typ av säkerhetsproblem kan knappast någon enskild aktör i tjänstekedjan sägas ha ett samlat ansvar. Det ankommer på säkerhetsföretagen att som en del av sin kommersiella etablering utveckla olika former av försvar mot illasinnad kod såsom antivirusprogram och mjukvarubrandväggar. Utvecklare av operativsystem och annan mjukvara med stor spridning har naturligtvis också ett ansvar att se till att mjukvaran de utvecklar i så stor utsträckning som möjligt är fri från brister från första början och, i den utsträckning så inte är fallet, att snabbt uppdatera mjukvaran och tillse att sådana uppdateringar effektivt når ut till allmänheten för att förhindra att säkerhetsbrister utnyttjas för att sprida illasinnad kod bland deras kunder.

Det som gör problemet med botnät något unikt är att koden i sig ofta inte skadar slutanvändaren direkt, eftersom nätverken vanligen utgör medel att utföra illasinnade aktiviteter mot andra (att jämföra med t.ex. ett virus som ofta direkt skadar informationen på slutanvändarens dator). Det finns därför möjligen inte heller samma incitament för slutanvändaren att åtgärda problemet och denne kan många gånger ha svårt att själv upptäcka problemet.

Varje drabbad slutanvändares Internetleverantör blir därmed också en väsentlig del i kedjan, inte bara vad avser själva smittotillfället utan även vad avser nyttjandet av botnätet för att utföra de illasinnade aktiviteterna. Internetleverantörer får därmed anses ha en mer särpräglad roll i problematiken kring botnät än i problematiken med illasinnad kod i allmänhet.

Nedan diskuteras kortfattat myndighetens syn på vilket ansvar som kan anses ligga under respektive roll.

5.1.2 Internetleverantörernas ansvar förändras med utvecklingen inom området

Utgångspunkten när det gäller Internets infrastruktur är att det är den tjänstetillhandahållare som sköter de elektroniska kommunikationstjänsterna som har ansvaret för sina nät och tjänsternas kvalité. En betydande del av ansvaret för infrastrukturen, även den logiska, ligger därmed hos Internetleverantörerna som inom ramen för vad som är kommersiellt möjligt

på en konkurrensutsatt marknad vidtar åtgärder för att skydda sina respektive delar mot störande eller förstörande incidenter. Problematiken med botnät är dock att den ofta inte drabbar den tjänsteleverantör i vars nät botarna huserar. Det kan till och med vara så att botnätet utvecklas särskilt för att störa denne så lite som möjligt, eftersom botnätet så att säga lever på att den som levererar kapaciteten till nätverket fortsätter att göra så. Det finns inte heller samma kommersiella skäl för tjänsteleverantören att vidta åtgärder som i samband med skräppost. Om alltför stor del av den e-post en Internetleverantör sänder ut består av skräppost finns en reell risk att leverantörer drabbas själva genom att svartlistas på någon av de skräppostlistor som finns och därigenom blockeras av andra Internetleverantörer. Detta är också ett av de främsta skälen som de intervjuade leverantörerna angivit för att vidta så pass ingripande åtgärder vad gäller hanteringen av skräppost.

Det finns flera aspekter av begreppet ansvar, och att känna sig ansvarig kan även vara att acceptera sin roll som en del i en kedja av aktörer och se till vilka åtgärder som är rimliga och värdefulla att vidta, såväl för att skydda sina egna kunder som att i möjligaste mån begränsa problemets spridning. Att acceptera sig som en del av det område som inte bara utsätts för problemen, utan även inom vilka problemen huserar, innebär rimligen ett naturligare utgångsläge för att överväga åtgärder mot problemen.

Leverantörer av Internettjänsten är kanske de aktörer som har den mest komplexa rollen ansvarmässigt i botnätsproblematiken. De har å ena sidan ett ansvar att tillhandahålla den tjänst de levererar på ett så effektivt sätt som möjligt. De har vidare uttalade skyldigheter i lagstiftning att säkerställa att deras kunders integritet upprätthålls på så sätt att de normalt inte kan behandla trafik eller trafikuppgifter hur som helst och att uppgifter knutna till abonnemang och enskilda meddelanden hemlighålls. Dessa skyldigheter tyder på en bild av leverantören såsom endast en leverantör av kommunikation, som således inte ska ta hänsyn till vad som kommuniceras eller av vem utan endast säkerställa kommunikationens fullbordan.

Verkligheten ser väldigt annorlunda ut idag än när grunderna för lagstiftningen skrevs på telekomområdet då elektronisk kommunikation främst bestod av fast telefoni och i andra hand mobil telefoni. Idag består en allt viktigare del av de elektroniska kommunikationstjänsterna av Internetkommunikation vilket också innebär en mer komplex bild på vad som egentligen utgör innehållet i en kommunikation. Tidigare torde större delen av kommunikationens innehåll utgöras av tal och till en mindre del datakommunikation, medan kommunikationsmängderna idag är tvärtom. Datakommunikation innebär också att allt mer av intelligensen i systemen förflyttas ut mot

slutanvändarutrustningen. Medan de terminaler som existerade under telelagens tid på 90-talet inte löpte någon större risk att drabbas av säkerhetsrelaterade problem, är dagens terminaler genomgående tekniskt mycket avancerade och därmed potentiellt sårbara.

Denna utvecklig har också påverkat såväl marknaden som lagstiftningen. Idag levererar alla stora Internetleverantörer säkerhetspaket där slutkunden ges tillgång till programvaror i form av antivirusprogram och mjukvarubrandväggar. Till nya kunder tillhandahåller de flesta leverantörer också trådlösa routrar som på olika sätt är förkonfigurerade vilka i praktiken utgör även en fysisk brandvägg mot användarens terminaler om de är korrekt konfigurerade.

Vad gäller lagstiftningen har denna också utvecklats, om än långsamt, i samma riktning. När lagen om elektronisk kommunikation infördes 2003 och ersatte telelagen återfanns ett särskilt kapitel vad avser integritet. I detta kapitel ges leverantören ett särskilt ansvar att se till att de uppgifter som behandlas skyddas och informera användare om de särskilda risker som finns och på vilka sätt riskerna kan avhjälpas. Det återfinns också regler kring förbud mot avlyssning vilket hindrar i princip all behandling av pågående kommunikation om inte behandlingen har till syfte att se till att kommunikationen fullföljs. Lagen föreskriver också att elektroniska kommunikationsnät och kommunikationstjänster ska uppfylla rimliga krav på god funktion och teknisk säkerhet, vilket medför krav på att leverantörer bedriver ett kontinuerligt och systematiskt säkerhetsarbete för att säkerställa en grundläggande nivå avseende främst uthållighet, tillgänglighet och driftsäkerhet.

5.1.3 Slutanvändare behöver hjälp för att kunna ta sitt ansvar

Slutanvändaren har betydande möjligheter att påverka såväl sin egen säkerhetsmiljö som sitt beteende vid användning av Internet. Det är naturligtvis därför också mycket viktigt att slutanvändare får bra och lättförståelig information om både risker och möjligheter med Internetanvändning i allmänhet såväl som säkerhetsrisker med botar.

Det torde dock vara uppenbart att en betydande del av kretsen användare aldrig kommer att ha eller vara intresserade av att få den tekniska insikt det ofta kräver för att förstå problemens djupare innebörd. Det är därför av mycket stor vikt att det finns enkla och lättanvända verktyg att tillgå för att höja säkerheten. Enligt myndighetens uppfattning räcker det dock inte bara att dessa verktyg finns tillgängliga för att de ska användas. Det är även av stor betydelse att dessa verktyg erbjuds eller tillhandahålls via någon som redan har

ett kundförhållande med användaren såsom exempelvis Internetleverantören eller försäljaren av terminalen (t.ex. datorn eller mobiltelefonen).

5.2 Åtgärder som bör vidtas

Även om en aktör kan anses ha del av ett gemensamt ansvar så uppkommer naturligtvis frågan om vilka konkreta åtgärder ansvaret innefattar.

I detta avsnitt avser myndigheten att kort kommentera de åtgärder som vidtas eller inte vidtas av Internetleverantörer. Målsättningen är att förtydliga myndighetens principiella inställning till de olika åtgärderna och även ge incitament för aktörer att vidta åtgärder och till fortsatta diskussioner. Det säger sig självt att utvecklingen av separata tjänster eller säkerhetsrelaterade åtgärder i första hand bör utvecklas av aktörerna själva. Men mot bakgrund av att frågeställningar uppstått i de intervjuer myndigheten haft finns det anledning att kommentera de olika åtgärderna.

Det ska även förtydligas att den analys som kan göras av de siffror myndigheten givits tillgång till, oavsett deras bristfällighet, inte kan bedömas som så alarmerande att några akuta åtgärder torde krävas. Däremot befarar PTS att ett betydande mörkertal med all säkerhet finns och att problemet på sikt kan bli allvarligare. Det torde ligga i alla parters intresse att åtgärder vidtas som kan förhindra eller i vart fall försvåra denna utveckling. Det torde även ligga i alla parters intresse att dessa åtgärders effektivitet och rimlighet diskuteras inbördes mellan olika parter, där även myndigheten kan ha en roll.

5.2.1 Direkt stöd till användarna är grundläggande

PTS är mycket positiva till utvecklingen att Internetleverantörer i stor utsträckning informerar om risker och även tillhandahåller antivirusprogram samt mjukvarubrandväggar som en del av kommunikationstjänsten. En sådan utveckling tyder på att aktörerna tar ansvar för sina användare och även klart tydliggör för sina kunder vikten med att upprätthålla ett rimligt skydd. Enligt PTS uppfattning bör denna typ av extratjänster kunna utvecklas och marknadsföras tydligare av berörda Internetleverantörer. Det är naturligtvis upp till marknadsaktörerna att själva avgöra inriktningen på deras marknadsföring, men PTS vill ändå särskilt uppmuntra leverantörerna att använda sig av budskap om säkra tjänster och det mervärde sådana tjänster kan ge.

Såsom redogjorts för ovan i avsnitt 4.1.4 tar vissa av Internetleverantörerna kontakt med de användare som blivit en del av ett botnät, medan andra inte gör så. Från PTS synvinkel ter det sig som en mycket viktig åtgärd att göra användare uppmärksamma på den situation de befinner sig i, oavsett den

ekonomiska kostnad detta kan innebära för Internetleverantören. Att ha kännedom om aktiva botnät men att välja att inte ta kontakt med drabbade användare, som vanligen har stora möjligheter att göra något åt problemet, kommer rimligen endast att innebära att problemet på sikt växer. Det finns förvisso möjligheter att på andra sätt hantera effekterna av ett botnät (t.ex. blockering av trafik), men det ter sig som en mycket viktig del att med alla rimliga medel ha ambitionen att problemen ska åtgärdas så nära källan som möjligt. Flera av leverantörerna har angivit ekonomiska skäl som anledningen till att man inte vidtar åtgärder och även att leverantören kan få en negativ stämpel. PTS har förståelse för den ekonomiska invändningen, att manuellt hantera all kontakt med användare är endast effektivt om antalet är förhållandevis litet. Det finns dock enligt PTS uppfattning all anledning för leverantörerna att överväga automatiska system för, i vart fall initieringen av, sådan kontakt. Beräkningar torde kunna göras avseende hur kostnaden för implementeringen av sådana system står sig jämfört med kostnaden för manuell hantering. Vad gäller den eventuella negativa stämpeln en leverantör skulle kunna ges anser PTS att denna åtgärd från leverantören istället borde kunna marknadsföras och vändas till något positivt. De leverantörer som faktiskt kontaktar sina kunder vittnar också om att den stora merparten kontaktade kunder endast är positiva till att de blivit uppmärksammade på problemet.

5.2.2 Branschen kan samverka kring principer för kundkontakter

Eftersom situationen är likvärdig för de flesta leverantörer finns det inom detta område stora möjligheter för marknaden att inom branschen komma överens om likvärdiga förhållningssätt om vilken typ av kontakt man ska ta, vilken dignitet en indikation om säkerhetsproblem en kund måste ha nått upp till för att medföra att kontakt tas samt vilka åtgärder som vidtas mot kunder som inte svarar på kontaktförsök. Om sådana förhållningssätt är likvärdiga inom branschen bör enskilda leverantörer ha mycket lättare att såväl ekonomiskt som motivationsmässigt bygga upp ett system för hantering av dessa situationer.

5.2.3 Övervakning av trafiken ger värdefull information

Trafikanalys och i övrigt kartläggning av trafik som efter signaturer kan uppfattas som kommunikation inom ett botnät ser PTS som mycket viktigt att genomföra *om* målet är att löpande kunna upprätthålla en realistisk bild av hur antalet datorer i Sverige som infekterats av en bot utvecklas. Att enbart förlita sig på uppgifter utifrån är inte tillräckligt för att få en realistisk bild. För att sådan information ska kunna bli jämförbar mellan olika Internetleverantörer och således kunna användas för att ge en större bild av utvecklingen inom Sverige krävs att analysen tillämpas enhetligt. Såsom redovisats ovan finns det

idag ingen möjlighet att göra bra jämförelser mellan de siffror som Internetleverantörer har uppgivit i intervjuer.

Det bör dock påpekas att i den utsträckning trafikanalysen utgör en behandling av innehållet i kommunikationen, i motsats till behandling av endast trafikuppgifter, måste utgångspunkten vara att användaren samtyckt till en sådan behandling. Flera av Internetleverantörerna har uttryckt tveksamheter om var gränsdragningarna går avseende lagstiftningen. Myndigheten återkommer till dessa frågor under avsnitt 6.4 nedan.

5.2.4 Blockering av trafik bör användas med försiktighet

Såsom redogjorts i avsnitt 2.3.2 kan blockering omfatta allt från total blockering av en användares Internetanslutning till partiell eller dynamisk blockering baserad på trafikanalys. Det är därför svårt att generellt uttala sig om blockering som sådan.

PTS anser dock sammanfattningsvis att blockering av trafik är ett verktyg som måste hanteras med viss försiktighet. Det är förvisso ett kraftfullt och mångsidigt verktyg men också något som kan upplevas som mycket negativt utifrån integritetsaspekter och möjligheten för individen att själv välja det sätt denne vill nyttja sin Internettjänst. I den utsträckning blockering används för att helt blockera portar som normalt inte används för kommunikation, ser PTS att det finns rimliga anledningar att vidta sådana åtgärder, såsom t.ex. skett avseende utgående e-posttrafik. Detta måste dock kombineras med tydlig information till användaren och även rimligen en möjlighet för användaren att i enskilda fall öppna upp blockeringen av portar om detta krävs för att användaren ska kunna nyttja den tjänst han avtalat om.

Det kan vara aktuellt att i enskilda fall blockera trafiken för användare vars dator infekterats med en bot, som en sista utväg om användaren inte förmått åtgärda problemet trots information från Internetleverantören. De leverantörer som har som praxis att ta kontakt med sina användare när botar upptäcks i nätet, har också genomgående angivit att de i sista hand är beredda att helt stänga av en användare men att det sällan behöver ske. PTS anser dock att denna hantering måste ske med försiktighet. Myndigheten har förvisso förståelse för behovet men anser att man även måste ta hänsyn till att användaren kanske inte återkommit för att denne inte förstår problemet själv. Systemet med att isolera en användare på så sätt att denna fortfarande har möjlighet att nyttja tjänster för uppgradering av operativsystem, genomsökning av terminalen efter illasinnad programvara, såsom virus/botar etc., är intressant. Det ger kunden en möjlighet att komma tillrätta med problemet

samtidigt som det effektivt begränsar möjligheten för en infekterad dator att användas som plattform för attacker.

Ett alternativ som kan vara intressant är att Internetleverantörer levererar en separat Internet-tjänst som i förhand endast tillåter sådan trafik som majoriteten av användarna har behov av. En sådan tjänst skulle kunna lanseras som en säkrare tjänst och tillhandahållas till en målgrupp som inte kräver några mer avancerade kommunikationstjänster över Internet. Vissa Internetleverantörer har antytt att de ser positivt på idén men angivit att de är tveksamma att genomföra den, eftersom tjänsten skulle kunna upplevas som ”sämre” än andras tjänster och därför ha sämre konkurrensmöjligheter.

Sannolikheten att en begränsning i tjänsten, såsom blockering av något slag, upplevs negativt av en användare, torde öka ju mindre den säkerhetsrisk som begränsningen avser att komma till rätta med framstår som påtaglig för användaren. Till skillnad från filtrering av skräppost – ett fenomen som de flesta upplever dagligen – är riskerna med botnät inte på samma sätt synliga och inte i första hand riktade mot de användare som berörs av begränsningarna i Internetleverantörens tjänst. I slutänden torde dock användares uppfattning av dylika begränsningar i stor utsträckning utgöra en marknadsföringsfråga.

6 Hur kan PTS driva arbetet vidare?

6.1 Myndighetens roll

PTS är sektorsmyndighet för elektronisk kommunikation, vilket även inbegriper Internet. PTS vision är att alla i Sverige ska få tillgång till effektiva, prisvärda och säkra kommunikationer. PTS har ett tillsynsansvar i enlighet med lagen (2003:389) om elektronisk kommunikation (LEK). Utgångspunkten för PTS arbete med kvalitet och säkerhet i elektroniska kommunikationer är att främja konkurrensen på marknaden, upphandling av säkerhetshöjande åtgärder, samverkan mellan stat och näringslivs samt reglering och tillsyn.

Myndighetens roller inom ramen för botnätsproblematiken kan vara flera. Löpande bedrivs arbete inom Sitic för att snabbt förmedla information och råd avseende aktuella säkerhetshot och inträffade incidenter, till såväl Internetleverantörer som andra myndigheter, företag och organisationer. I denna rapport har myndigheten rollen som undersökande i syfte att få en uppfattning om hur problematiken ser ut i Sverige. PTS har också som ambition att rapporten ska belysa några av de problem som är speciella avseende botnät och då särskilt den ansvarfördelning och skillnader i ambition och uppfattning om vilka åtgärder som är rimliga att vidta inom ramen för tillhandahållandet av en Internettjänst.

Som angivits ovan är myndighetens främsta medel för att uppnå lagstiftningens mål avseende säkerhet att främja konkurrens mellan Internetleverantörerna även inom detta område. Det är en målsättning att säkerhetsfrågor ska kunna utgöra en konkurrensaspekt som kan leda till att aktörer som hanterar säkerhet bättre också får konkurrensfördelar. Det kan dock inte med säkerhet sägas att det finns en sådan utveckling inom detta område. Botnätsproblematiken är, såsom redogjorts för ovan, också något speciell i det att den sällan i första hand drabbar den användare som faktiskt infekterats, eller den leverantörs nät som huserar många botar hårdast.

PTS har tidigare, inom ramen för strategin för ett säkrare Internet i Sverige, uttalat en stående ambition att möjliggöra och även tydliggöra Internetleverantörers möjlighet och ansvar att värna om sina användares säkerhet. I denna rapport har PTS konstaterat att även om inställningen till problematiken till botnät är likartad bland Internetleverantörer så finns det betydande skillnader mellan aktörernas ambition när det gäller att vidta åtgärder kring problemet. PTS ser följande avsnitt som en redogörelse för möjliga aktiviteter myndigheten kan vidta inom området. Myndigheten har som

ambition att vidare undersöka området och vidare bedöma vilka möjliga aktiviteter det finns anledning att gå vidare med.

6.2 Förbättrade metoder för att mäta utvecklingen

För att kunna erhålla en entydig bild över botnätsutbredningen i Sverige, som kan ligga till grund för en bedömning som är mer tillförlitlig än vad som varit möjligt inom ramen för föreliggande rapport, så kan PTS konstatera att vedertagna mätmetoder skulle behöva etableras och tillämpas av samtliga större Internetleverantörer, så att samma typ av mätning utförs under en och samma tidsperiod.

Ytterligare utredning krävs, för att kunna bedöma hur omfattande det arbete skulle vara, som krävs för att införa sådan automatiserad mätning. Som ett initialt steg torde det dock vara möjligt för Internetleverantörer att, med tillämpning av en gemensam metod, över tiden föra statistik över den förekomst av botar de själva görs varse om, oavsett hur dessa uppgifter kommit till leverantörens kännedom. Som konstaterats ovan, är det ingen av de Internetleverantörer PTS intervjuat som har uppgivit att de idag sammanställer sådan statistik.

Myndigheten skulle i detta sammanhang kunna samla svenska Internetleverantörer och initiera det samarbete som krävs för att etablera sådana gemensamma mätmetoder.

6.3 Referensgrupp kring problematiken

Samtliga av de aktörer PTS samtalat med vid framtagandet av rapporten har varit positiva till närmare samtal aktörerna emellan avseende problematiken. På Internetleverantörssidan förekommer förvisso mer eller mindre informella samtal på teknisk nivå kring detta och andra problem, dock inte i någon regelbunden eller organiserad form.

Myndigheten skulle därför kunna ha en sammankallande roll och anordna en referensgrupp där frågorna kan diskuteras. I gruppen bör såväl Internetleverantörer som säkerhetsföretag och berörda branschorganisationer delta. Blad de intervjuade aktörerna har det dock framförts skilda meningar avseende vilka personer som bör delta i en sådan referensgrupp. Vissa har ansett att sådana möten måste besökas av representanter av en förhållandevis hög nivå, som kan ta beslut på policynivå, medan andra anser att samtalsformen skulle vara enklare om gruppen bestod av mer teknisk orienterad personal. Det kan därför finnas anledning att låta gruppens deltagare variera, beroende på vilka specifika frågor som ska diskuteras.

Såväl Internetleverantörers som säkerhetsföretags syn på problematiken skulle kunna utgöra en mångfacetterad grund, från vilken både spridningen i sig men också möjliga och effektiva åtgärder skulle kunna diskuteras. Som redovisats i rapporten tidigare har flera av aktörerna sagt sig vara intresserade av idén att lansera tjänster med fokus på säkerhet men ansett att konkurrensen är ett problem då dessa tjänster kan ses som mer begränsade än andra. Utgångspunkten för en referensgrupp bör vara att enbart diskutera problem och åtgärder, med en målsättning att komma fram till gemensamma angreppssätt och åtgärder.

6.4 Förtydliganden och förändringar av de rättsliga förutsättningarna för åtgärder

Ett flertal av aktörerna har angivit att frågetecken föreligger kring de rättsliga förutsättningar för att vidta åtgärder såsom trafikanalys, begränsning i åtkomsten till Internet m.m. Mot bakgrund av den osäkerhet som verkar föreligga på marknaden finns det anledning för PTS att förtydliga och kommunicera de nu föreliggande rättsliga förutsättningarna för främst Internetleverantörer att vidta åtgärder i syfte att kartlägga och stävja problemet med botnät.

PTS har tidigare genom regeringsuppdraget *Strategi för ett säkrare Internet i Sverige* föreslagit lagändring vad avser filtrering av elektronisk kommunikation som angriper och äventyrar Internettjänsten eller nätets funktion. Någon sådan lagändring har ännu inte övervägts av regeringen. PTS har emellertid för avsikt att förnya frågan om lagändring till stöd för Internetleverantörers arbete med att förebygga och åtgärda uppkomna säkerhetsproblem i nätet. PTS målsättning är en tydlig reglering som väl balanserar skyddet för användarnas personliga integritet mot behovet av att upprätthålla säkerheten, såväl i nätet i sin helhet som för enskilda användare.

6.5 Webbplats för jämförelse av säkerhet

I samarbete med Konsumentverket tillhandahåller PTS webbplatsen Telepriskollen som hjälper konsumenten att jämföra priser och villkor mellan olika operatörer inom fast och mobil telefoni samt bredband, mobilt och uppringt Internet. Uppgifterna om priser och andra villkor kommer från operatörerna själva och kontrolleras av PTS.[20] Internetleverantörer har till olika delar de senaste åren lanserat allt fler säkerhetsprodukter tillsammans med sina Internettjänster. För att ytterligare motivera marknaden och därigenom stödja utvecklingen av konkurrens om inte bara pris utan även om tjänstekvalitet och

[20] Se http://www.telepriskollen.se/. PTS tillhandahåller även webbplatser som hjälper användare att hitta på säkra lösenord (https://www.testalosenord.se/) och att testa sin dators säkerhetsnivå (https://www.testadatorn.se/).

säkerhetsnivåer, skulle PTS kunna utveckla den befintliga jämförelsetjänsten eller lansera en liknande webbplats där leverantörernas säkerhetstjänster översiktligt skulle kunna redovisas.

Litteratur

1. PTS rapporter

Individundersökningen 2008 - Svenskarnas användning av telefoni och Internet (2008). (PTS-ER-2008:24)

Spionprogram och andra närliggande företeelser (2005). (PTS-ER-2005:15)

Strategi för ett säkrare Internet i Sverige (2006). (PTS-ER-2006:12)

2. Andra rapporter

F-secure Corporation (2008). *F-Secure IT Security Threat Summary for the Second Half of 2008*.

Krisberedskapsmyndigheten m.fl. (2005) *Botnets, Nulägesbeskrivning, 2005-09-27*..

OECD (Organisation for Economic Co-operation and Development) (ännu ej publicerad), *Communications Outlook 2009*.

Symantec Corporation (2008). *Symantec Report on the Underground Economy, July-07 – June-08*.

Bilaga 1

Organisationen ShadowServer

ShadowServer är en organisation som bildades år 2004 och består av säkerhetsspecialister som på frivillig basis bedriver informationsinsamling, analys, övervakning och informationsspridning avseende illasinnad kod, botnät och bedrägerier på nätet. ShadowServer har som mål att förbättra säkerheten på Internet genom att öka medvetenheten om sådana hot.

ShadowServer använder följande tillvägagångssätt för att söka efter botnät.

- Användning av honungsfällor som samlar på den illasinnade kod som överförs från angripande datorer.
- Chattprogram används för att fånga upp länkar i reklammeddelanden som skickas till användarna och som pekar till filer innehållande illasinnad kod.
- Länksökningar, dvs. genomgång av forum och sökmotorer efter nyckelord som är relevanta för kända varianter av illasinnad kod.

När illasinnad kod har lokaliserats, genomförs en analys av den insamlade koden för att utröna mekanismen för tillträde till botnätet. När Shadowserver har tagit reda på kommunikationsprotokollen och lokaliserat ledningsnoden påbörjas övervakningen av botnätet med hjälp av en testdator med mjukvara som är anpassad för att imitera en dator som infekterats med en bot. Tanken är att angriparen ska se testdatorns mjukvara som en vanlig bot i sitt nätverk. Den anpassade mjukvaran loggar dock enbart botnättrafiken, utan att utföra otillåtna uppgifter som en riktig bot hade gjort.

Mer information om ShadowServer finns på http://www.shadowserver.org.