Sentor MSS AB
IT-säkerhet 24x7

DDos Attacker

Niklas Blomquist
Regionchef/Senior Security Consultant

HK
Stockholm

Regionkontor
Malmö
London

sentor

Agenda

- Kort om Sentor
- Vad är en DoS attack
- Lite historik om DoS och DDoS attacker
- Olika typer av DoS och DDoS attacker
- Verktyg som förövaren använder sig av
- Vad kan man göra för att skydda sig?

Vilka är Sentor?

- Levererar IT-säkerhet
- Övervakning & Respons 24/7
- Säkerhetsanalyser/IT-Brottsutredning
- Incidenthantering/Metodik för säkerhetsarbete
- Omvärldsbevakning/R&D

Niklas Blomquist

- Senior Security Consultant
- Mer än 10 års erfarenhet
- Uppdrag inom:
  - Säkerhetsanalyser
  - Rådgivning
  - Design av säkerhetslösningar
  - Granskning/revidering
  - Expertvittne i IT-Brottsmål

Vad är en DoS attack?

Vad är en DoS attack

- Denial of Service
- Överbelastningsattack
- Gjord för att konsumera alla tillgängliga resurser
  - Kan vara riktad mot:
    - Infrastruktur
    - Servrar
    - Applikationer
    - Backendsystem

Vad är en DoS attack

- Överbelastningsattack
  - Kan vara riktad mot:
    - CPU
    - Bandbredd Internet
    - Statetabeller i brandväggar
    - Serieinterface på routrar
    - Minne i webbservrar
    - O.s.v.

Historik om DoS och DDoS attack

Historik om DoS och DDoS attack

- Historiskt är det välkända sajter som drabbats
  - Yahoo
  - Amazon
  - Microsoft
- Attackeraren har främst varit ute efter uppmärksamhet och/eller bekräftelse i hackerkretsar

Historik om DoS och DDoS attacker

- Idag är det främst företag i starkt behov av/eller som har ekonomisk vinning av sin Internetnärvaro
- Motiven idag är främst finansiella, men även politiska/religiösa
- DDoS är idag det vanligaste sättet

Olika former av attacker

Olika former av attacker

- DoS
- DDoS

Olika former av attacker

- DoS
  - Överbelastningsattack
  - Kan vara riktad mot:
    - Infrastruktur
    - Servrar
    - Applikationer
    - Backendsystem
  - En dator skickar trafik till den ”utvalda” sajten
  - Kräver mycket bandbredd och/eller vissa svagheter i infrastrukturen för att lyckas
- DDoS

Olika former av attacker

- DoS
- DDoS
  - Överbelastningsattack
  - Kan vara riktad mot:
    - Infrastruktur
    - Servrar
    - Applikationer
    - Backendsystem
  - Många datorer skickar trafik till den ”utvalda” sajten
  - Från 1000 till 1 000 000 datorer
  - Trafikmängden justeras så rätt mängd trafik används
  - Ökas resurserna på den ”utvalda” sajten, ökas trafikmängden

Olika tekniker för att utföra attacker

Olika tekniker för att utföra attacker

- SYN flood
- ACK flood
- UDP flood
- ICMP flood

Olika tekniker för att utföra attacker

- SYN flood
  - TCP baserad attack
  - SYN -> SYN ACK -> ACK
  - Skickar bara SYN och låter sessionen tajma ut
  - Skickar 10.000, 100.000 eller 1 000 000 tals SYN per sekund
  - Vanligen är attackerna styrda så precis lagom mycket trafik skickas, om mer resurser frigörs så skickas mer trafik
- ACK flood
- UDP flood
- ICMP flood

Olika tekniker för att utföra attacker

- SYN flood
- ACK flood
  - I stället för att skicka SYN paket, som många har försvar mot, skickas ett ACK.
  - Routern, brandväggen etc. kommer att spendera CPU tid på att utvärdera huruvida detta är en befintlig koppling eller något fel

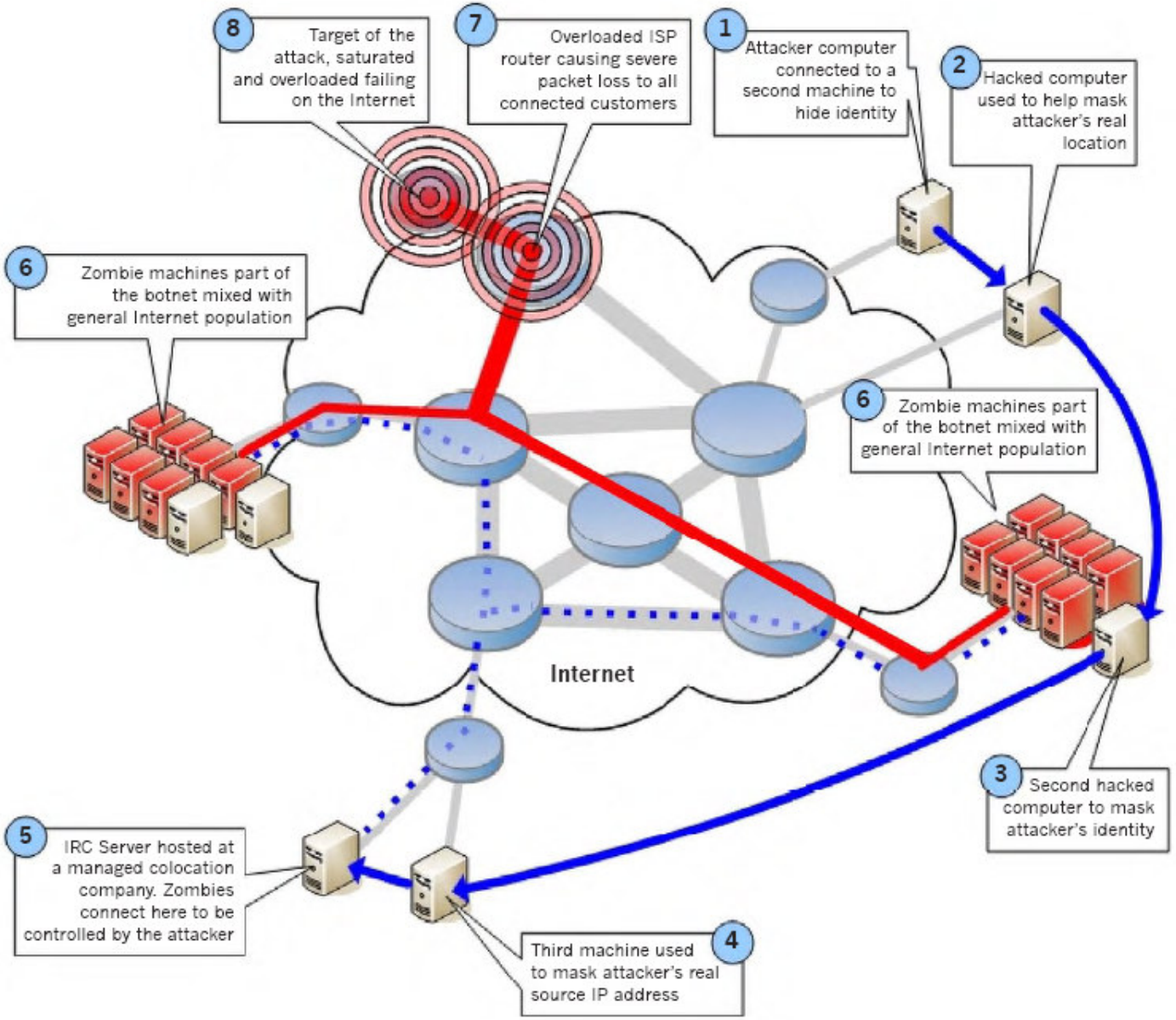
- UDP flood
- ICMP flood

Olika tekniker för att utföra attacker

- SYN flood
- ACK flood
  - I stället för att skicka SYN paket, som många har försvar mot, skickas ett ACK.
  - Routern, brandväggen etc. kommer att spendera CPU tid på att utvärdera huruvida detta är en befintlig koppling eller något fel
- UDP flood
  - Används för att konsumera all tillgänglig bandbredd
  - Vanligen används starkt fragmenterade paket för att överlasta routrar och brandväggar
- ICMP flood

Olika tekniker för att utföra attacker

- SYN flood
- ACK flood
- UDP Flood
- ICMP flood
  - Används för att konsumera all tillgänglig bandbredd


8
Target of the attack, saturated and overloaded failing on the Internet
7
Overloaded ISP router causing severe packet loss to all connected customers
1
Attacker computer connected to a second machine to hide identity
2
Hacked computer used to help mask attacker's real location
6
Zombie machines part of the botnet mixed with general Internet population
6
Zombie machines part of the botnet mixed with general Internet population
Internet
3
Second hacked computer to mask attacker's identity
5
IRC Server hosted at a managed colocation company. Zombies connect here to be controlled by the attacker
4
Third machine used to mask attacker's real source IP address

Verktyg

Verktyg

- Första generationens verktyg
- Andra generationens verktyg
- Tredje generationens verktyg

Verktyg

- Första generationens verktyg
  - Mycket enkla verktyg
  - Command-line
  - Exekveras på en maskin
  - *SYNC, Flood*
- Andra generationens verktyg
- Tredje generationens verktyg

Verktyg

- Första generationens verktyg
- Andra generationens verktyg
  - Client – Server verktyg
  - Möjliggör styrning av många maskiner samtidigt
  - Hackas in manuellt
  - *stacheldraht, trinoo och tfn*
- Tredje generationens verktyg

Verktyg

- Första generationens verktyg
- Andra generationens verktyg
- Tredje generationens verktyg
  - Client-server
  - Möjlighet att sprida sig själv
  - Utökade möjligheter att styra attacker och anpassa trafikmängd
  - Utökade möjligheter att uppdatera sig själv
  - Utökade funktioner för undgå upptäckt av anti-virus

Verktyg

- Trojan funnen vid analys
- Controll – Efter installation kopplar den upp sig mot en icke-publik IRC kanal eller via http
- Installation – Möjlighet att sprida sig till datorer i närheten genom utnyttja sårbarheter
- Klarade SYN och UDP Flood
- Klarar även filöverföring (via FTP, TFPT, HTTP, IRC etc.)
- Tangentbordsavlyssning, portscanner osv

Dagens hotbild eller exempel, tagna från verkligheten

Attack mot regeringen

Regeringens hemsida släcktes av nätpirater i natt i en andra attackvåg.
Även polisens sajt sänktes på nytt och låg tidigt på söndagen fortfarande nere.
Vid åttatiden i morse kom regeringens hemsida igång igen.

Statsminister Göran Persson fick tidigt i morse information om att regeringens hemsida slocknat.

Persson vill inte kommentera händelsen. Inte heller om han fått uppgifter som tyder på att attacken kan ha med razzian mot Pirate Bay att göra.

– Jag vågar inte spekulera om det, svarar Persson enligt TT.

Samma mönster som tidigare

Myndighetssveriges viktigaste hemsida släcktes strax före midnatt.

I morse arbetade regeringens säkerhets- och it-avdelning febrilt med att starta upp den igen, och vid åttatiden på söndagsmorgonen gick det åter att surfa in på sajten.

Attacken följde samma mönster som angreppet på polisens hemsida, som låg nere i nästan ett dygn innan den under en kort tid var uppe igen.

En anonym hemsida skapades - och på olika diskussionsforum uppmanades sedan alla deltagare att gå in på den.

Alla som besöker sajten deltar automatiskt i attacken mot regeringens hemsida.

På sajten finns dessutom en kort text där justitieminister Thomas

Hemsidan släckt - på tio sekunder

Det här är sajten som skapades för att utföra attacken.

4 dagar av nätkrig

- I onsdags stängdes sökmotorn The Pirate Bay efter en landsomfattande polisrazzia.
- I torsdags kom svaret i form av en attack mot polisens hemsida, som kraschade.
- Polisens sajt låg nere i nästan ett dygn för att sedan komma upp igen. I går kväll släcktes den dock ingen.
- I går kväll attackerades dessutom regeringens hemsida, som nu ligger nere.

- "Jag sparar en tusenlapp i månaden på att fildela"
Trebarnsmamman Cecilia skulle vilja betala - men branschen

Säpo utreder attack mot regeringens hemsida

Krisberedskapsmyndigheten: Svenska myndigheter har inte insett riskerna för IT-attacker

Regeringens hemsida låg nere i åtta timmar.
Nu utreder Säpo attacken både mot regeringens och polisens hemsida.
Krisberedskapsmyndigheten anser att svenska myndigheter inte tillräckligt har insett riskerna för IT-attacker.

Regeringens webbplats låg nere från midnatt till åttatiden på söndagsmorgonen.

Regeringskansliet meddelade på eftermiddagen att man polisanmält händelsen och att man nu samarbetar med polisen för att lösa problemet på längre sikt.

Regeringens hemsida bombarderades under natten med tre gånger fler anrop än tidigare rekord, som är den höga belastning man har då budgetpropositionen läggs ut.

Enligt regeringskansliets it-tekniker har någon gjort en hemsida avsedd att överbelasta regeringen.se.

- Skälet var att en extern webbsajt har skickat automatiska anrop mot en specifik fil på regeringskansliets webbplats, säger Hanna Brogren, informationschef vid regeringskansliet, till TT.

Enligt polisen finns också misstankar om att uppkopplade datorer kapats via virusprogram för att delta i attacken utan att datorägaren har en aning om det.

Regeringskansliet samarbetar nu bland annat med polisen för att försvåra nya attacker mot hemsidan.

Säpo utreder

Under söndagseftermiddagen lämnade kansliet in en anmälan till Säpo.

- Vi har fått in en anmälan om att vi ska utreda om det varit en eventuell åtgärd riktad mot regeringskansliets webbplats, säger Anders Thornberg, informationsdirektör vid Säpo.

Han säger att Säpo kommer att utreda anmälan parallellt med Rikskriminalpolisens utredning av attacken mot polisens hemsida som låg nere tidigare under veckan.

Angreppet mot polisens webbplats rubriceras som grovt egenmäktigt förfarande, det finns ännu ingen person misstänkt.


Thomas - vi vill ha tillbaka våran frihet!
Polisen har gjort en razzia mot The Pirate Bay och Piratbyrån. Läs mer på följande sidor:
DN
Piratbyrån
TV4
SVT
DN
Expressen
Bara genom att ha den här sidan öppen i din webbläsare visar du vad du tycker om MPAAs bluff, Thomas Bodström!

Hur gick det till?

- Förövaren letade upp den största filen på webbplatsen.
- Ett script skapades som laddade ner filen i bakgrunden
- Scriptet publicerades på en webb-sida
- Länken till sidan spreds via olika chatforum och e-mail
- Det tog 10 minuter i planering och genomförande att göra polisens hemsida obrukbar

Hur vanligt är det med DoS/DDoS attacker?

Hur vanligt är det med DoS/DDoS attacker?

- Mörkertalet är mycket stort
- Enligt 2006 CSI/FBI Computer Crime
  - 25% av de svarade hade varit med om en DDoS attack
- Uppskattningar är gjorda till över 10 000 attacker om dagen!

Hur vanligt är det med DoS/DDoS attacker?

- Attackerna blir större och större
  - 2005 var den största attacken 3,5 Gbps
  - 2006 var den största attacken 10Gbps
- Med denna tillgängliga bandbredd kan en attackerare ta ut hela ISP’er och hosting/co-locations
- Det största Zoombienätet är över 1 000 000 st datorer.

Sentors erfarenheter

Trender

- Baseras på
  - 8 års 24x7 intrångsövervakning
  - Omvärldsbevakning
  - Mer än 1000 säkerhetsanalyser och IT-brottsutredningar
  - Kundgrupp
    - Myndigheter
    - Globala företag och organisationer
    - Börsnoterade företag

Vad ser vi?

Trender

- Attacker kommer ofta från ekonomiskt svaga regioner
- Attackerna har gått från ”bara för skojs skull” till kriminell aktivitet
- Hot och utpressning har funnits i alla tider, nu även på Internet
- Attackerarna och deras verktyg blir mer och mer avancerade
- Vi har sett indikationer på en ny våg av DDoS attacker

Hur skyddar man sig?

Hur skyddar man sig?

- Är man mindre beroende av sin Internetnärvaro
  - IPS
  - Utökad åtgärd via sin ISP
  - Accesslistor i routrar
  - Manuella åtgärder, t.ex. byte av ip-adress på webbservrar
  - Ingen av ovanstående åtgärder är fullgoda

Hur skyddar man sig?

- Är man beroende av sin Internetnärvaro
  - Filtrera all trafik på OSI lager 3-7
  - Filtrera all ”icke önskvärd trafik” hos ISP
  - Protokollverifiering hos ISP
  - Applikationslagerfiltrering hos ISP
  - Signaturverifiering hos ISP
  - Anomaliverifiering hos ISP
  - Plan för adaptiv attack
- Garanterad bandbredd från t.ex. Prolexic

Frågor?

Tack för er tid!

- Niklas Blomquist
- Sentor MSS AB
- niklas.blomquist@sentor.se
- 073 – 600 49 77