

# Storskaliga attacker mot infrastruktur

fredrik söderblom  
xpd systems ab  
fredrik@xpd.se





# Vad gör din son vid datorn?

# Agenda



- Historia
- Nutid
- Hur fungerar det?
- Vem drabbas?
- Vem/vilka ligger bakom?
- Kan man skydda sig mot DoS/DDoS?

# Historia



- DoS attacker
  - Överbelastningsattack
  - Denial Of Service
- Olika typer av överbelastningsattacker
  - Ping-Of-Death ..
  - Teardrop (fragmenteringsattack)
  - land (samma host/port)
  - smurf/fraggle (reflektorattack)
  - SYN flood
  - etc

# Historia



- SYNflood
- Projekt Neptune
- Idé och koncept av Michael Schiffman (aka daemon9)
  - 1:a September 1996
  - "proof-of-concept" kod i Phrack 48, kapitel 13
  - Ej praktiskt fungerande kod, vitala delar var bortkommenterade

# Förändringar och motdrag



- Företag och individer började skydda sig själva och sina applikationer
- Patchade IP stackar
- SYN cookies et al
- Cisco's TCP Interceptor

# Förändringar och motdrag



- Slutligen kom någon på genidraget :)
  - Behöver vi egentligen attackera enskilda maskiner eller applikationer?
  - Nej. Varför anstränga sig?
  - Fyll deras serieförbindelse till deras ISP istället ..

# Förändringar och motdrag



- Alternativt, skjut så mycket paket att deras loggande brandvägg snurrar runt och dör istället.
  - Lika effektivt, och ibland till och med effektivare ..



# Förändringar och motdrag



- Fråga
  - Hur får vi ihop till bandbredden som behövs?

# Förändringar och motdrag



- Distribuera attacken :)
- Såsom en klassisk 3-lagers distribuerad klient/server applikation
  - Medför dessutom som extra grädde på moset ett extra lager av skydd för den som genomför attacken
  - Se till att klienten är självreplikerande så att den infekterade basen kan bli större

# Förändringar och motdrag



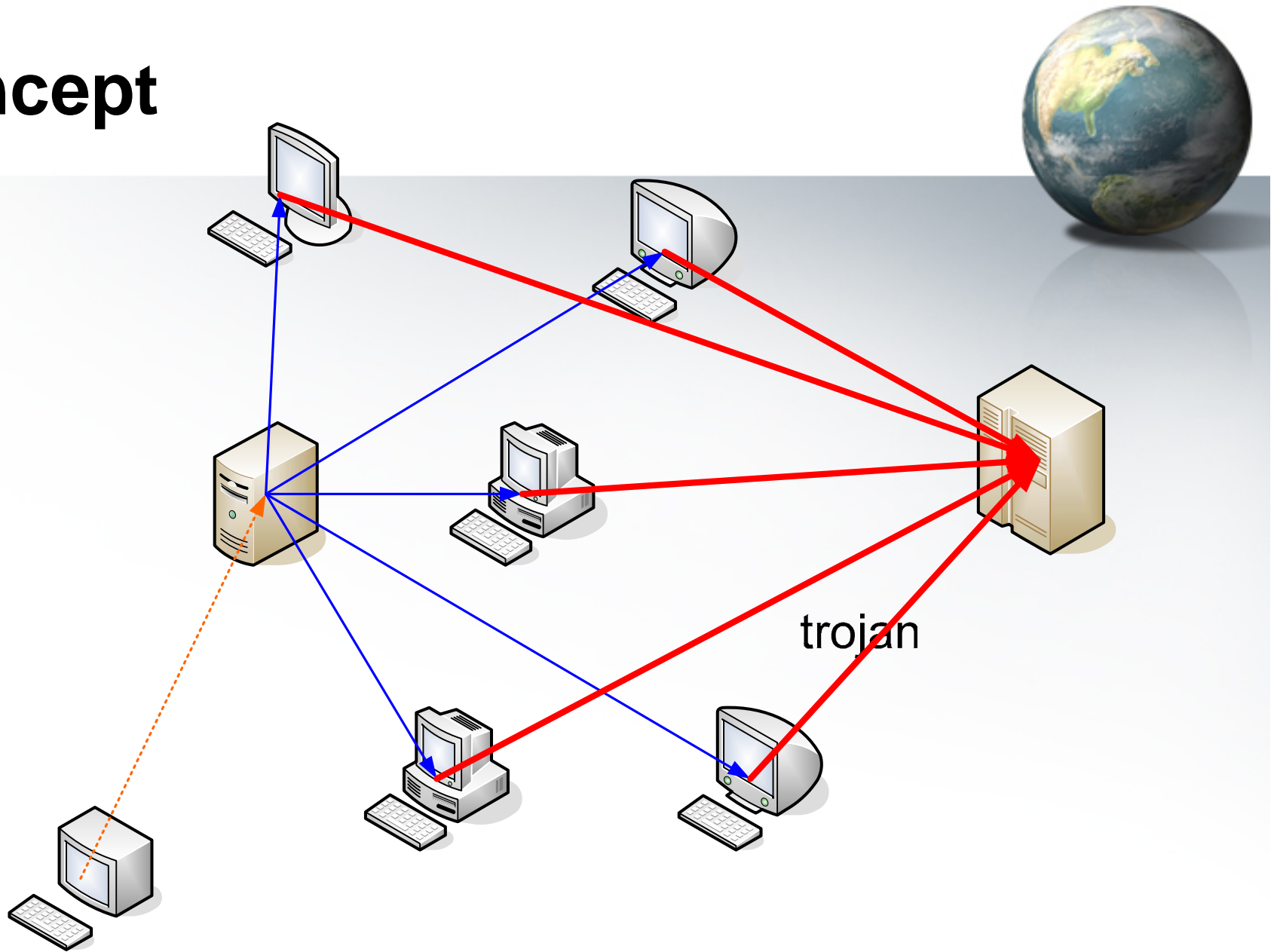
- Säg hej till "DDoS attacker"
  - Distributed Denial Of Service
- Idé
  - Infektera många klienter (100-10 000)
  - Fjärrstyr dem
- Verkan
  - Dränk offrets serielina med skräp
  - Eller överbelasta hans/hennes router eller brandvägg

# Motdraget



- 1999
  - trinoo
  - Tribe Flood Network (TFN)
    - TFN2K
  - stacheldracht
  - Shaft
  - ...

# Konzept



# Den listige



```
- PuTTY
22:06:52.816964 69.93.247.82.33237 > 213.131.131.150.45: udp 10 (DF)
22:06:52.816968 69.93.247.82.33237 > 213.131.131.150.45: udp 10 (DF)
22:06:52.816990 69.93.247.82.33237 > 213.131.131.150.45: udp 10 (DF)
22:06:52.816993 69.93.247.82.33237 > 213.131.131.150.45: udp 10 (DF)
22:06:52.816996 69.93.247.82.33237 > 213.131.131.150.45: udp 10 (DF)
22:06:52.817000 69.93.247.82.33237 > 213.131.131.150.45: udp 10 (DF)
22:06:52.817033 69.93.247.82.33237 > 213.131.131.150.45: udp 10 (DF)
22:06:52.817052 69.93.247.82.33237 > 213.131.131.150.45: udp 10 (DF)
22:06:52.817056 69.93.247.82.33237 > 213.131.131.150.45: udp 10 (DF)
22:06:52.817103 69.93.247.82.33237 > 213.131.131.150.45: udp 10 (DF)
22:06:52.817106 69.93.247.82.33237 > 213.131.131.150.45: udp 10 (DF)
22:06:52.817129 69.93.247.82.33237 > 213.131.131.150.45: udp 10 (DF)
22:06:52.817132 69.93.247.82.33237 > 213.131.131.150.45: udp 10 (DF)
22:06:52.817172 69.93.247.82.33237 > 213.131.131.150.45: udp 10 (DF)
22:06:52.817295 69.93.247.82.33237 > 213.131.131.150.45: udp 10 (DF)
22:06:52.817460 69.93.247.82.33237 > 213.131.131.150.45: udp 10 (DF)
22:06:52.817465 69.93.247.82.33237 > 213.131.131.150.45: udp 10 (DF)
22:06:52.817487 69.93.247.82.33237 > 213.131.131.150.45: udp 10 (DF)
22:06:52.817565 69.93.247.82.33237 > 213.131.131.150.45: udp 10 (DF)
22:06:52.817569 69.93.247.82.33237 > 213.131.131.150.45: udp 10 (DF)
22:06:52.817629 69.93.247.82.33237 > 213.131.131.150.45: udp 10 (DF)
22:06:52.817633 69.93.247.82.33237 > 213.131.131.150.45: udp 10 (DF)
22:06:52.817785 69.93.247.82.33237 > 213.131.131.150.45: udp 10 (DF)
--More-- (31%)
```

# Den dumme

A screenshot of a PuTTY terminal window. The title bar reads "PuTTY". The terminal content consists of 17 lines of network traffic logs, each starting with a timestamp and showing a packet being sent from 64.225.121.11.32866 to 213.131.131.150.6667 via UDP port 900, with a "DF" (Destination Full) status. At the bottom of the terminal, there is a status bar that says "--More-- (56%)".

```
20:39:19.408902 64.225.121.11.32866 > 213.131.131.150.6667:  udp 900 (DF)
20:39:19.408978 64.225.121.11.32866 > 213.131.131.150.6667:  udp 900 (DF)
20:39:19.409055 64.225.121.11.32866 > 213.131.131.150.6667:  udp 900 (DF)
20:39:19.409136 64.225.121.11.32866 > 213.131.131.150.6667:  udp 900 (DF)
20:39:19.409210 64.225.121.11.32866 > 213.131.131.150.6667:  udp 900 (DF)
20:39:19.409287 64.225.121.11.32866 > 213.131.131.150.6667:  udp 900 (DF)
20:39:19.409364 64.225.121.11.32866 > 213.131.131.150.6667:  udp 900 (DF)
20:39:19.409441 64.225.121.11.32866 > 213.131.131.150.6667:  udp 900 (DF)
20:39:19.409521 64.225.121.11.32866 > 213.131.131.150.6667:  udp 900 (DF)
20:39:19.409597 64.225.121.11.32866 > 213.131.131.150.6667:  udp 900 (DF)
20:39:19.409674 64.225.121.11.32866 > 213.131.131.150.6667:  udp 900 (DF)
20:39:19.409750 64.225.121.11.32866 > 213.131.131.150.6667:  udp 900 (DF)
20:39:19.409827 64.225.121.11.32866 > 213.131.131.150.6667:  udp 900 (DF)
20:39:19.409905 64.225.121.11.32866 > 213.131.131.150.6667:  udp 900 (DF)
20:39:19.409982 64.225.121.11.32866 > 213.131.131.150.6667:  udp 900 (DF)
20:39:19.410061 64.225.121.11.32866 > 213.131.131.150.6667:  udp 900 (DF)
20:39:19.410175 64.225.121.11.32866 > 213.131.131.150.6667:  udp 900 (DF)
20:39:19.410243 64.225.121.11.32866 > 213.131.131.150.6667:  udp 900 (DF)

--More-- (56%)
```



# Gammal skåpmat



```
- PuTTY
14:08:31.469548 IP 219.167.2.130.3702 > 213.131.131.155.22963: UDP, length: 801
14:08:31.469751 IP 212.244.46.163.2764 > 213.131.131.155.15242: UDP, length: 801
14:08:31.469821 IP 219.176.98.100.1221 > 213.131.131.155.2102: UDP, length: 801
14:08:31.469889 IP 211.20.99.130.4108 > 213.131.131.155.7429: UDP, length: 801
14:08:31.469967 IP 12.213.187.221.4297 > 213.131.131.155.31336: UDP, length: 801
14:08:31.470038 IP 204.101.150.8.4236 > 213.131.131.155.28885: UDP, length: 807
14:08:31.470107 IP 211.187.245.94.3617 > 213.131.131.155.537: UDP, length: 801
14:08:31.470178 IP 218.163.84.128.1544 > 213.131.131.155.6940: UDP, length: 807
14:08:31.470246 IP 218.16.84.254.3896 > 213.131.131.155.25860: UDP, length: 801
14:08:31.470316 IP 219.21.38.34.3308 > 213.131.131.155.25145: UDP, length: 801
14:08:31.470386 IP 211.227.46.36.3405 > 213.131.131.155.20030: UDP, length: 801
14:08:31.470456 IP 213.107.78.133.1049 > 213.131.131.155.21380: UDP, length: 801

14:08:31.466251 IP 219.39.246.15.2121 > 213.131.131.155.2571: UDP, length: 801
0x0000: 4500 033d 3f1f 0000 6a11 e43a db27 f60f E..=?...j...'.
0x0010: d583 839b 0849 0a0b 0329 e06f 2b20 2b20 .....I...) .o+.
0x0020: 2b41 5448 302b 202b 202b 4154 4830 2b20 +ATH0+...+ATH0+
0x0030: 2b20 2b41 5448 302b 202b 202b 4154 4830 +.+ATH0+...+ATH0
0x0040: 2b20 2b20 2b41 5448 302b 202b 202b 4154 +.+ATH0+...+AT
0x0050: 4830 2b20 2b20 2b41 5448 302b 202b 202b H0+...+ATH0+...+
0x0060: 4154 4830 2b20 2b20 2b41 5448 302b 202b ATH0+...+ATH0+.
0x0070: 202b 4154 4830 2b20 2b20 2b41 5448 302b .+ATH0+...+ATH0+
0x0080: 202b 202b 4154 4830 2b20 2b20 2b41 5448 .+.+ATH0+...+ATH
0x0090: 302b 202b 202b 4154 4830 2b20 2b20 2b41 0+...+ATH0+...+A

--More-- (91%)
```



# Enklare matematik



- Av 1000 slumpmässigt utvalda Windows användare, så har merparten (80-90%) av dem
  - Ingen personlig brandvägg (Och ingen förståelse varför dem skulle behöva en heller iofs :)
  - Inget Antiviruskydd (Samma oförståelse här, tyvärr)
- Skapa en trojan som aktiveras genom klickning
- Sprid denna URL via MSN, email, ICQ, IRC och eventuellt några öppna forum.

# Enklare matematik



- Så snart trojanen är på plats så försöker den självreplikera genom kända attackvektorer (MS-DCOM et al)
- Inom en relativt kort tid så kommer vi att ha ett så kallat "botnet" på mellan 500 och 1000 trojaner
- Som vi kan fjärrstyra totalt
- Frågor? :)

# Resultat



- Telia ADSL
  - Erbjuder sina kunder ca 500Kbps upp och ned
  - I detta fall bryr vi bara om "upp"
  
  - 10 trojans \* 0.5 (teoretisk max Mbps) = 5 Mbps
  - 100 trojans \* 0.5 (teoretisk max Mbps) = 50 Mbps
  - 1000 trojans \* 0.5 (teoretisk max Mbps) = 500 Mbps

# Resultat



- Bostream
  - Erbjuder privatkunder upp till 26Mbps upp och ner
  - 10 trojaner \* 26 (teoretisk max Mbps) = 260 Mbps
  - 100 trojaner \* 26 (teoretisk max Mbps) = 2.6 Gbps
  - 1000 trojaner \* 26 (teoretisk max Mbps) = 26 Gbps

# Resultat



- Bredbandsbolaget
  - Erbjuder privatkunder upp till 100 Mbps upp och ner
  - 10 trojaner \* 100 (teoretisk max Mbps) = 1 Gbps
  - 100 trojaner \* 100 (teoretisk max Mbps) = 10 Gbps
  - 1000 trojaner \* 100 (teoretisk max Mbps) = 100 Gbps
- Nu är det rätt tid att oroa sig :)

# Nutid



- Dagens DDoS trojaner/klienter använder IRC som "master" servrar (se tidigare slides)
  - Privata/stängda IRC servrar på hackade maskiner
  - Publika IRC servrar
- Det sistnämnda gör det ännu enklare att infektera ännu fler



# Kort IRC Primer

# Kort om IRC



- IRC - Internet Relay Chat
- Skapades 1988 av
  - Jarkko Oikarinen, Oulu universitetet i Finland
- Beskrivs av RFC1459
- RFC1459 uppdateras av RFC2810 – RFC2813
  - Dock så använder i princip alla RFC1459



# Kort om IRC



- Som en gigantisk telefonkonferens
  - Men all kommunikation sker via text
  - Man väljer själv vilka man pratar med
  - antingen en och en i taget
    - /msg pelle Hur gick det på provet igår?
  - eller så grupperar man ihop flera deltagare i en så kallad kanal:
    - #linux, #motorcyklar, #ridning

# IRC nät



- Det finns drygt 800 publika IRC nät
  - Med cirka 1.3 miljoner dagliga användare
  - Som samsas om 646 495 kanaler
  - På cirka 5 570 IRC servrar

# Exempel



X-Chat [1.8.11]: froo @ wineasy2.se.quakenet.org / #sec-heads (+ptncCk...)

X-Chat Windows User Modes Settings Scripts & Plugins User Menu Help

OS Security has taken the red pill, but has yet to realize how deep the rabbit hole goes

[10:49] <falfa> prim0: har ni tittat på att stoppa in stackskydd i några av era servrar?  
[10:49] <falfa> Ahnberg: tjena!  
[10:58] @prim0> falfa såsom ?? vi kör grsec på våra linux burkar  
[11:02] <falfa> som t.ex. <http://www.tri.ibm.com/projects/security/ssp/>  
[11:03] <falfa> Anledningen till att jag frågar är att jag tycker det låter nervöst att stoppa in  
[11:03] <falfa> stacksmashprylar i en produktionsmiljö och undrar hur ni resonerat.  
[11:04] <falfa> grsec gör väl lite annat än skyddar stacken?  
[11:14] @prim0> japp  
[11:20] @prim0> vi har inte riktigt titta på detta, vi kör som sagt grsec men den ger ingen stackskydd  
[11:20] @prim0> känns som om det är för tidigt att köra i prod miljö  
[11:33] <falfa> prim0: man vill ju helt klart testa det långsamt och under en längre tid för att känna att det fungerar  
[11:54] @prim0> precis  
[12:14] wineasy2.se.quakenet.org sets modes [#sec-heads +ooo falfa lmn smp]  
[14:43] @Ahnberg> Tjenare. :)  
[15:22] @falfa> :)  
[15:22] @falfa> Ahnberg: kommer du den 19:e?  
[16:22] [join] thomass (~none@...telia.com) has joined #sec-heads  
[16:28] @Ahnberg> falfa: jag har tänkt det.  
[16:28] @Ahnberg> Jag är iofs dubbelbokad, så jag vet inte hur jag ska lösa det. Men jag har tänkt försöka. :)  
[16:28] @Ahnberg> Det är en utbildning jag ska på, kan förmodligen skippa dag 2.  
[17:28] [quit] Ahnberg has quit (Ping timeout)  
[21:41] <oorf> ehem  
[21:41] <oorf> grsec ger ju stackskydd  
[21:44] [nick] You are now known as froo  
[21:44] <froo> smile, you are on candid camera

ep  
falfa  
froo  
L  
lmn  
MobRules  
prim0  
smp  
thomass

Voice DeVoice  
Banlist Kick  
Send Dialog  
Lookup Whois

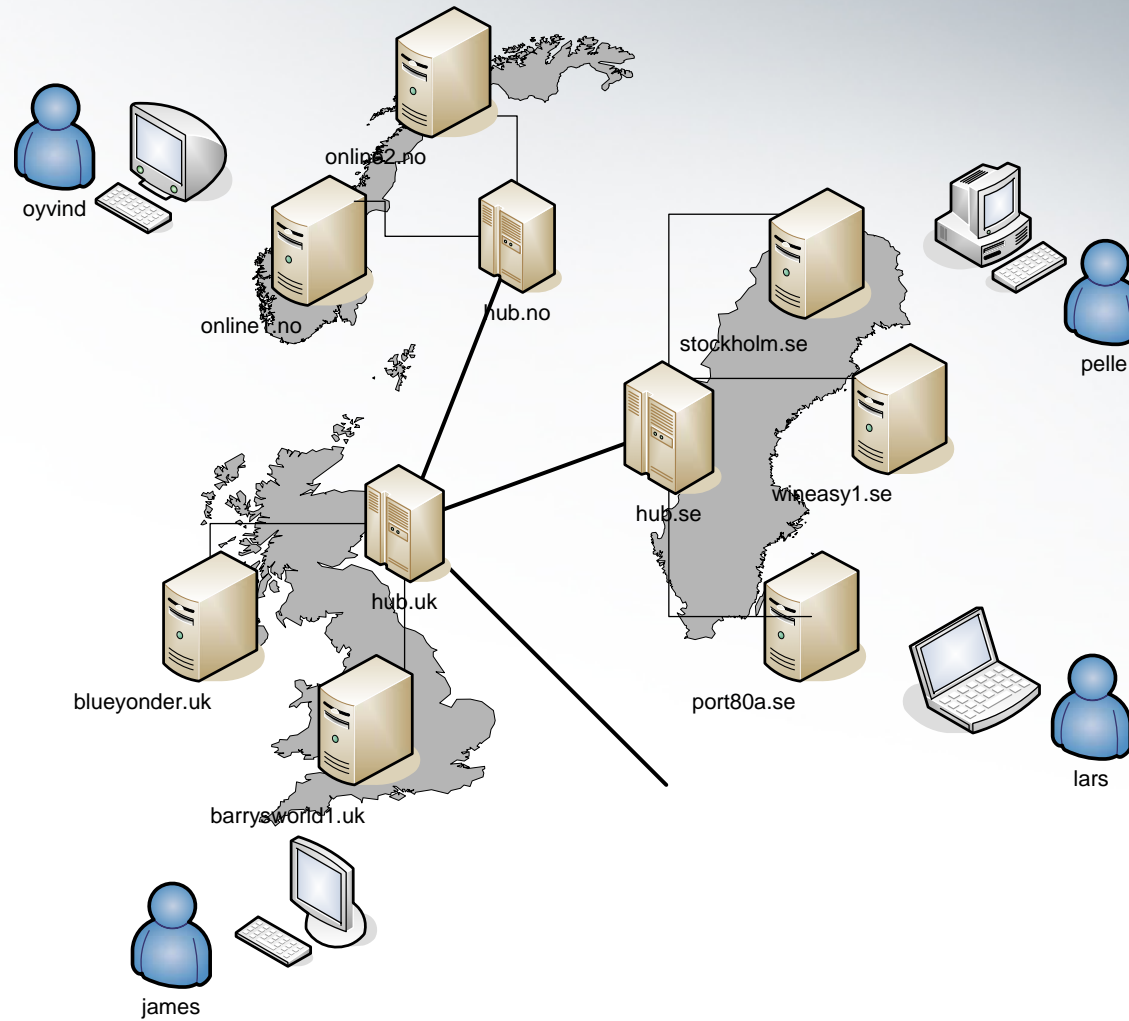
wineasy2.. (gline) (kill) (splits) Q O S L N (snotices) (notices) #snails #rtfm #rtfm-priv #nbrigad.. #wineasy #we.staff #sec-heads #twiligh... #se-opers #qnet.st..

# IRC Struktur



- IRC servrar
- IRC hubbar
- IRC operatörer
- Kanaler (rum)
- Klienter

# IRC Struktur



# Operatörer



- Administrerar nätverket
  - Länkar och slår ihop nätet efter behov
- Hjälper användare tillrätta, dvs traditionell support
  - #feds
  - #help

# Operatörer



- Kan också avskilja användare som inte följer nätets AUP eller regler
  - Antingen temporärt genom att avbryta klientens förbindelse till nätet mha en sk KILL
  - Eller permanent med en global ban (en sk GLINE), som kommer att stänga hela nätet för en eller flera IP adresser



# The Big Five



- QuakeNet
  - Ett IRC nät av gamers för gamers
  - Startades 1997 i Sverige/Danmark
  - ca 240 000 samtidiga användare
  - ca 90 operatörer
  - ca 50 servrar i 9 länder
    - Sverige, Danmark, Norge, Finland
    - England, Tyskland, Nederländerna
    - Italien och Irland



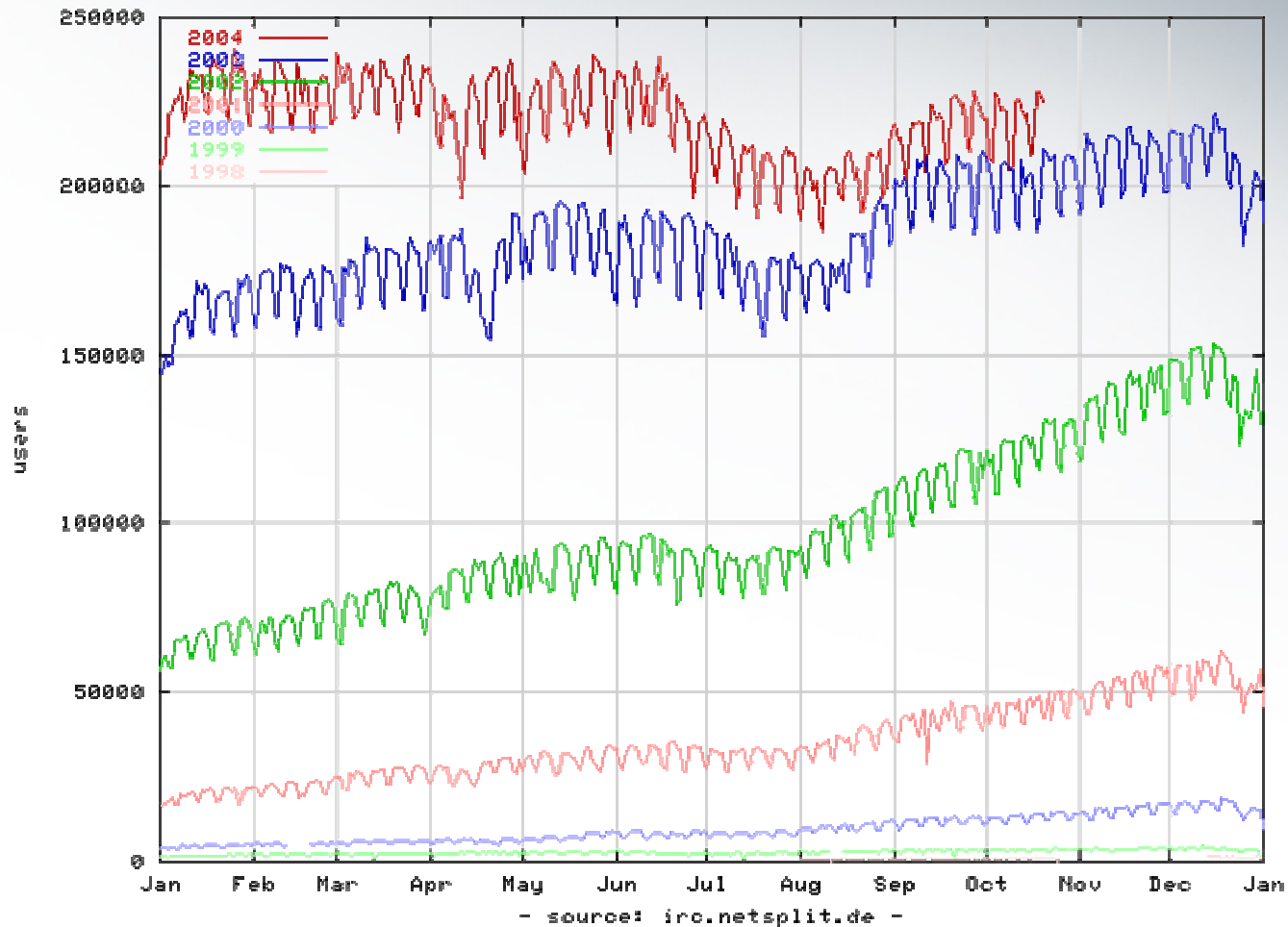


# The Big Five



- QuakeNet avviker en smula från traditionella IRC nät
  - Följande är inte tillåtet och tolereras inte:
    - Spridning av illegalt material (mp3, filmer, kopior av programvara etc)
    - pornografi
    - Rasism/Nazism
    - Hacking/Cracking

# QuakeNet



# The Big Five



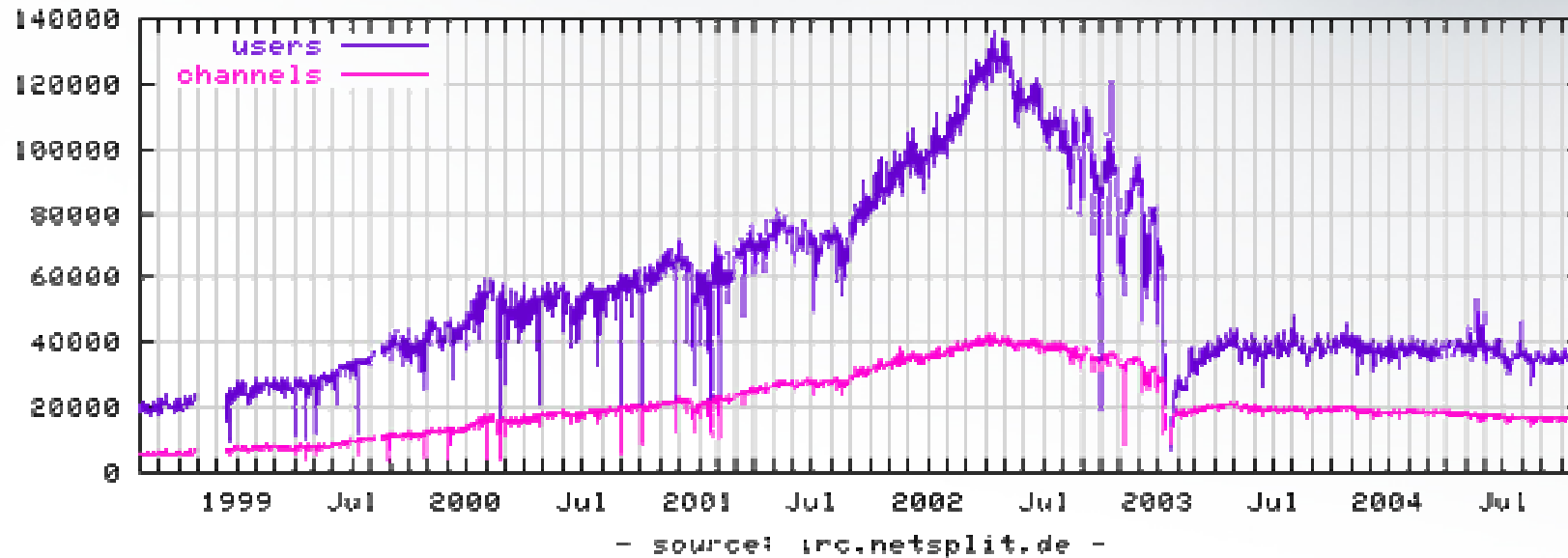
- UnderNet
  - ca 160 000 samtidiga användare
  - ca 100 operatörer
- EFnet
  - ca 140 000 samtidiga användare

# The Big Five



- IRCnet
  - ca 126 000 samtidiga användare
- DALnet
  - ca 40 000 samtidiga användare
  - ca 140 000 (före DDoS)

# DALnet



# IRC baserade trojaner



- spybot
- sdbot
- gh3tt0spy
- mIRC baserade trojaner
- mfl ..

# IRC baserade trojaner



- Många klienter har inbyggd replikering
  - utnyttjar kända attackvektorer, tex MS DCOM
- Och som bonus, lite inbyggda bakdörrar
  - Keystroke loggers
  - Skärmdumpar
  - Filöverföring
  - Uppdatering

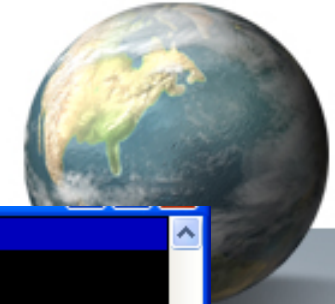
# Hur gör man?



- Välj ut en lämplig klient från ett relativt stort utbud av tillgängliga trojaner
- Konfigurerar klienten
  - Vilken IRC server, port, kanal, passord etc
- Kompilera och paketera den
- Sprid den som vilket virus som helst
  - IE, email, ICQ, MSN etc



# Dokusåpa



```
22:06 | -!- G-Anna37 [MULTIMEDIA@roskilde-66-33.ip-pluggen.com] has joined #sapultra
22:07 | -!- G-Max83 [Max83@213.66.36.155] has quit irc (Ping timeout)
22:10 | -!- G-walle98 [~walle98@h120n2fls31o841.telia.com] has quit irc (Ping timeout)
22:11 | -!- G-apwpbv [apwpbv@h101n1fls31o1001.telia.com] has joined #sapultra
22:13 | -!- Marklund [~M@hej.alla.kom.och.lek.med.oss.som.har.sparc.se] has joined #sapultra
22:13 | -!- Marklund [~M@hej.alla.kom.och.lek.med.oss.som.har.sparc.se] has left #sapultra ()
22:15 | -!- G-Christina10 [~Christina@h190n2c2o1029.bredband.skanova.com] has joined #sapultra
22:23 | -!- G-Mange30 [~Mange30@t5o950p33.telia.com] has quit irc (Ping timeout)
22:24 | -!- G-Bertil83 [~Bertil83@t9o922p28.telia.com] has joined #sapultra
22:24 | -!- G-Max16 [Max16@h155n1fls31o823.telia.com] has joined #sapultra
22:25 | -!- G-Christina10 [~Christina@h190n2c2o1029.bredband.skanova.com] has quit irc (Read
error: Connection reset by peer)
22:26 | -!- G-Hel [COMPUTER17@t2o30p102.telia.com] has joined #sapultra
22:27 | -!- G-l-g93 [~l-g93@t2o65p39.telia.com] has quit irc (Read error: Connection reset by peer)
22:35 | -!- G-Magnus47 [Magnus47@klover103.bitnet.nu] has joined #sapultra
22:36 | -!- Marklund [~M@hej.alla.kom.och.lek.med.oss.som.har.sparc.se] has joined #sapultra
22:36 | < Marklund> !login ██████████
22:36 | < Marklund> !syn 213.67.226.203 6667 1 1000
22:36 | < G-Max16> SynFlooding: 213.67.226.203 port: 6667 delay: 5 times:1000.
22:36 | < G-Helen84> SynFlooding: 213.67.226.203 port: 6667 delay: 5 times:1000.
22:36 | < G-HP-Auktoriser> SynFlooding: 213.67.226.203 port: 6667 delay: 5 times:1000.
22:36 | < G-apwpbv> SynFlooding: 213.67.226.203 port: 6667 delay: 5 times:1000.
22:36 | < G-Leifsson10> SynFlooding: 213.67.226.203 port: 6667 delay: 5 times:1000.
22:36 | < G-Seppo70> SynFlooding: 213.67.226.203 port: 6667 delay: 5 times:1000.
22:36 | < G-Bertil83> SynFlooding: 213.67.226.203 port: 6667 delay: 5 times:1000.
22:36 | < G-Anna37> SynFlooding: 213.67.226.203 port: 6667 delay: 5 times:1000.
22:36 | < G-KiD86> SynFlooding: 213.67.226.203 port: 6667 delay: 5 times:1000.
22:36 | < G-Hel> SynFlooding: 213.67.226.203 port: 6667 delay: 5 times:1000.
[02:45] [██████████] [2:#sapultra(+nst)]
[#sapultra] █
```

# Mål



- ebay, yahoo
- IRC nät
- Vanliga hemanvändare
- webbsajter

# Profil



- Vanligtvis en 13 till 20 årig pojke/man
- Dagens trojaner kräver minimal kunskap
  - Vilket syns allt som ofta :)
- En dator med internetaccess
- Dvs, relativt många potentiella kandidater

# Varför?



- Huvuddelen av fallen
  - Vanlig hederlig vandalism
  - Maktkänsla
  - Utlöses ibland av det som förövaren uppfattar som brist på respekt
  - Kan börja med en dispyt i ett onlinespel, på IRC, ICQ eller liknande

# Varför?



- En minoritet (än så länge)
  - Utpressning
  - Rökridå för annan attack/intrång
  - Pengar (relativt nytt fenomen)
    - SPAM

# Hur skyddar man sig mot DDoS?



- Det finns (än så länge i alla fall) ingen "patentlösning" på problemet
- Släng bandbredd på problemet
  - Räcker dock inte vid större attacker
  - Såvida man inte har väldigt mycket bandbredd

# Hur skyddar man sig mot DDoS?



- Abuserapportera alla attacker
  - SITIC
  - Kräver någon form av loggning
    - Tcpdump, snoop et al
    - Vesa Virta's (FRA) FIFO lösning
    - Cisco Netflow
  - I bästa fall så kommer 5-10% av trojanerna att försvinna permanent

# Hur skyddar man sig mot DDoS?



- BGP anycasting
  - skyddar (vissa) root namnservrar
  - Kan vara svårt att implementera för vissa typer av applikationer
- Nullrouting vid provider edge
  - Kom överens med transit/peer om vilka BGP communities som används för nullrouting
  - Alternativt ha en väl förberedd plan på hur man ska agera, beslutsvägar, telefonnummer till providers etc



# Hur skyddar man sig mot DDoS?



- ratelimitering
  - ICMP är en bra start
- pushbackd
  - Steve Bellovin et al
  - fortfarande i draft
  - kräver support från tex Cisco, Juniper

# Hur skyddar man sig mot DDoS?



- Traceback
  - Stefan Savage
  - Steve Bellovin
    - RFC draft
- OpenSource lösningar
  - Linux, Zebra, iptables
  - OpenBSD, Zebra alt. SecureBGP, pf

# Hur skyddar man sig mot DDoS?



- Separat router
  - BGP (eget AS) alt. OSPF
  - separat IP block
  - om den blir attackerade så slutar den annonsera AS eller nät
- Kommersiella lösningar
  - Riverhead (numera Cisco)

# Praktiska tips



- Stäng av loggning i brandvägg
  - Inte en bra permanentlösning
  - Kanske kan hjälpa dig igenom det värsta ..
- Överväg BGP anycasting
- Använd ratelimitering
  - De flesta behöver inte mer än 10Mbps ICMP :)
- Filterera bort oönskade protokoll vid provider edge
  - om applikationen enkom använder TCP, så droppa alla andra protokoll (utom ICMP packet-to-big et al)

# Hur skyddar man sig mot infektion?



- Personlig brandvägg
  - XP har en rudimentär, men ok brandvägg
    - Dock inte påslagen i SP1 (och tidigare)
    - Brandväggen i SP2 är något bättre
  - ZoneAlarm (ägs av Checkpoint numera)
  - Tiny Personal firewall etc

# Hur skyddar man sig mot infektion?



- NAT wlan/router/firewall
  - D-Link
  - Netgear
  - mfl

# Hur skyddar man sig mot infektion?



- Uppdaterad antivirusapplikation
  - AVG (gratis för personligt bruk)
    - [www.grisoft.com](http://www.grisoft.com)
  - Norton, Symantec
  - F-Prot et al

# Hur skyddar man sig mot infektion?



- Automatisk uppdatering av Windows
  - [windowsupdate.microsoft.com](http://windowsupdate.microsoft.com)
- Använd **INTE** Internet Explorer
  - Senaste versionen har 20 opatchade buggar ...
  - Alternativ kan vara
    - Mozilla Firefox
    - Opera



# Hur skyddar man sig mot infektion?



- Cisco
  - supportar en egen utökning av 802.1x för att kunna forcera uppdaterat antiviruskydd mm
  - om klienten inte uppfyller ställda kriterier så kan den dirigeras om till ett uppdaterings VLAN
- Checkpoint har en liknande lösning
  - SCV, Secure Client Verification

# Hur väl rustade är vi?



- Inte speciellt, tyvärr..
- Huvudelen (80-90%) av alla med fast uppkoppling förstår inte behovet av
  - antiviruskydd
  - någon form av brandvägg

# Hur väl rustade är vi?



- Eller så har de helt enkelt aldrig hört talas om det
- En vanlig ursäkt är "Varför skall jag skydda mig? Jag har inget av värde på min dator"

# Slut



- Frågor?

# Referenser



- <http://www.phrack.org>
- <http://staff.washington.edu/dittrich/misc/trinoo.analysis>
- <http://staff.washington.edu/dittrich/misc/tfn.analysis.txt>
- <http://staff.washington.edu/dittrich/misc/stacheldraht.analysis.txt>

# Referenser



- [http://packetstormsecurity.com/distributed/TFN2k\\_Analysis-1.3.txt](http://packetstormsecurity.com/distributed/TFN2k_Analysis-1.3.txt)
- <http://www.research.att.com/~smb/papers/pushback-impl.pdf>
- <http://www.grisoft.com>
- <http://www.mozilla.org/products/firebird/>

# Referenser



- <http://www.opera.com>
- <http://www.riverheadnetworks.com>
- [http://www.noc.kth.se/utbildning/pdf/svensson\\_hakan\\_03063.pdf](http://www.noc.kth.se/utbildning/pdf/svensson_hakan_03063.pdf)
- <http://netsplit.de>

# Referenser



- <http://www.quakenet.org>
- <http://www.quakenet.org/rules>
- <http://www.mirc.com>
- <http://www.xchat.org>



# Referenser



- <ftp://ftp.rfc-editor.org/in-notes/rfc1459.txt>
- [http://www.irc.org/history\\_docs/jarkko.html](http://www.irc.org/history_docs/jarkko.html)
- <http://www.sitic.se>
- <http://www.fra.se>
- <http://www.sigsecurity.se>