Viren, Würmer und anderes Ungeziefer

- Was? Warum?
- Angriffsflächen eines Computers
- Würmer, Viren, Trojanische Pferde
- Hoaxes
- Spam
- Wie schützen?
- Sober.P / Q
- Links

Was ist das eigentlich?

- Viele Emotionen, wenig Wissen
  - > 90% wissen, dass sie gefährdet sind
  - < 10% schützen sich richtig
- Es sind auch nur Programme
- Sie werden von Menschen geschrieben und ausgesetzt

Warum?

- Motivation
  - „Befriedigung“ des Schreibers
  - Seit Sommer '01 Basis für Tausch von copyrightetem Material
  - Seit Herbst '03 Aufbau von Spam-Netzwerken
- Ziele
  - Keine Zerstörung des Computers
  - Normalerweise kein Datendiebstahl
  - Backdoors, sammeln von E-Mail Adressen

Angriffsflächen

- Jeder Computer ist „Server“
- Computersoftware enthält Fehler
  - 1 Fehler pro 1000 Zeilen Code
  - WinXP hat 40'000'000 Zeilen
  - Werden oft spät entdeckt
- Benutzer arglos
  - Klick auf Attachements, Links
  - Keine Passwörter, keine Sicherheitsupdates

Würmer

- Würmer verbreiten sich selbständig
- Würmer benötigen Computer-Schwachstellen
- Letzte Epidemie im Sommer '03

Viren

- Viren brauchen einen Wirt
  - Diskette
  - Dokument
  - E-Mail
- Viren müssen „angestossen“ werden
  - Meist durch den Benutzer

Trojanische Pferde

- Trojaner verstecken sich in „nützlichen“ Programmen
- Beispiel Adware

Spam

- Werbung
- „Nur“ ärgerlich
- Machen 60% ~ 90% des Mailaufkommens aus

Hoaxes

- Kein Virus, sondern die Warnung über einen fiktiven Virus
- „Bitte schicke mich all Deinen Bekannten“

Wie schützen?

- Updates
- Virenscanner (aktuell halten!)
- Firewall
- Bewusster Umgang mit E-Mails, Webseiten, Software
- Windows vermeiden?!?
- IE vermeiden!!!

Sober.P / Q

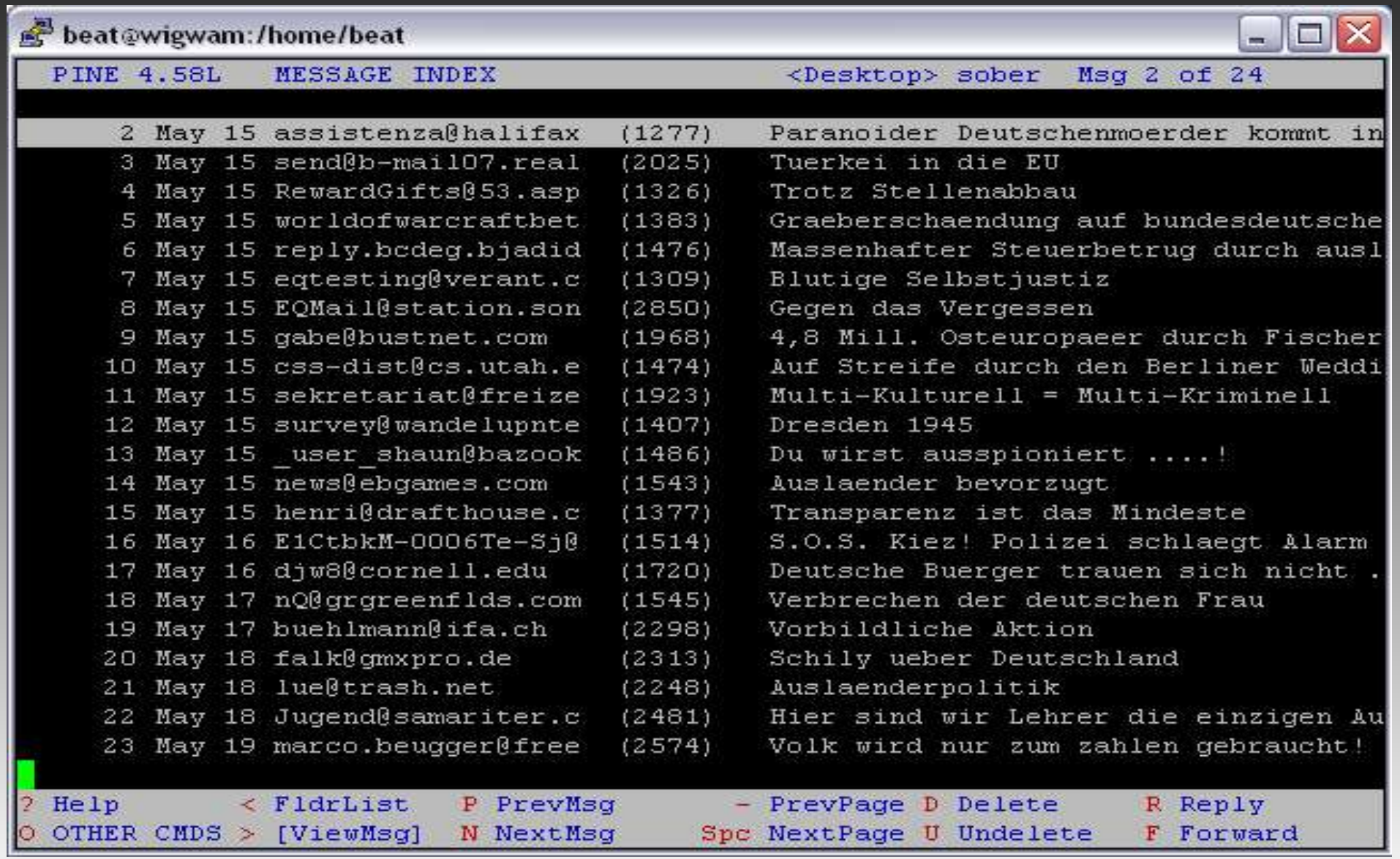
- Montag, 2. Mai: Erste Infektionen
- Dienstag, 3. Mai: In der Presse
- Freitag, 13. Mai: Ende Infektionen
- Samstag, 14. Mai: Start Spamming (Pfingsten)
- Samstag, 22. Mai: Ende Spamming, Versand des Nachfolgers

Sober.P / Q

beat@max:/home/beat

```
Date: Mon, 02 May 2005 16:10:09 GMT
From: Gewinn@fifa.de
To: esmooth777@lugs.ch
Subject: FwD: Glueckwunsch: Ihr WM Ticket

Herzlichen Glueckwunsch,

beim Run auf die begehrten Tickets für die 64 Spiele der Weltmeisterschaft
2006
in Deutschland sind Sie dabei.

Weitere Details ihrer Daten entnehmen Sie bitte dem Anhang.

Ihr "ok2006" Team
St. Rainer Gellhaus

--- FIFA-Pressekontakt:
--- Pressesprecher Jens Grittner und Gerd Graus
--- FIFA Fussball-Weltmeisterschaft 2006
--- Organisationskomitee Deutschland
--- Tel. 069 / 2006 - 2600
--- Jens.Grittner@ok2006.de
--- Gerd.Graus@ok2006.de

**** AntiVirus: Kein Virus gefunden
**** "LUGS" AntiVirus Service
**** WebSite: http://www.lugs.ch

    [ Part 2, Application/OCTET-STREAM (Name: "Fifa_Info-Text.zip")  ]
    [ 73KB. ]
```

Sober.P / Q


beat@wigwam:/home/beat
PINE 4.58L MESSAGE INDEX <Desktop> sober Msg 2 of 24
2 May 15 assistenza@halifax (1277) Paranoider Deutschenmoerder kommt in
3 May 15 send@b-mail07.real (2025) Tuerkei in die EU
4 May 15 RewardGifts@53.asp (1326) Trotz Stellenabbau
5 May 15 worldofwarcraftbet (1383) Graeberschaendung auf bundesdeutsche
6 May 15 reply.bcdeg.bjadid (1476) Massenhafter Steuerbetrug durch ausl
7 May 15 eqtesting@verant.c (1309) Blutige Selbstjustiz
8 May 15 EQMail@station.son (2850) Gegen das Vergessen
9 May 15 gabe@bustnet.com (1968) 4,8 Mill. Osteuropaeer durch Fischer
10 May 15 css-dist@cs.utah.e (1474) Auf Streife durch den Berliner Weddi
11 May 15 sekretariat@freize (1923) Multi-Kulturell = Multi-Kriminell
12 May 15 survey@wandelupnte (1407) Dresden 1945
13 May 15 _user_shaun@bazook (1486) Du wirst ausspioniert ....!
14 May 15 news@ebgames.com (1543) Auslaender bevorzugt
15 May 15 henri@drafthouse.c (1377) Transparenz ist das Mindeste
16 May 16 E1CtbkM-0006Te-Sj@ (1514) S.O.S. Kiez! Polizei schlaegt Alarm
17 May 16 djw8@cornell.edu (1720) Deutsche Buerger trauen sich nicht .
18 May 17 nQ@grgreenflds.com (1545) Verbrechen der deutschen Frau
19 May 17 buehlmann@ifa.ch (2298) Vorbildliche Aktion
20 May 18 falk@gmxpro.de (2313) Schily ueber Deutschland
21 May 18 lue@trash.net (2248) Auslaenderpolitik
22 May 18 Jugend@samariter.c (2481) Hier sind wir Lehrer die einzigen Au
23 May 19 marco.beugger@free (2574) Volk wird nur zum zahlen gebraucht!
? Help < FldrList P PrevMsg - PrevPage D Delete R Reply
O OTHER CMDS > [ViewMsg] N NextMsg Spc NextPage U Undelete F Forward

Sober.P / Q

- beat@rubis.ch meine alte Adresse:
  - 33 Vireneinschläge, einer bevor Antivirensoftware up to date war
  - > 500 Spammails
  - > 10'000x als Absender missbraucht

Links

- http://www.0x1b.ch/misc/papers/viren/
- http://www.tu-berlin.de/www/software/hoaxlist.shtml
- http://vil.nai.com/vil/content/v_133409.htm
- http://windowsupdate.microsoft.com/