Was ist Virus? - Ein Überblick !



- Was sind Viren ?
- Herausforderung
- Aktuelle Entwicklungen

- *Malware* (*Malicious Code*)

  Per Definition schädliche Software. Durch Medienberichte von der Öffentlichkeit oft mit „Viren“ gleichgesetzt

- *Viren* sind sich selbst replizierende, infizierende Dateien,

  In Relation zur Malware kaum noch verbreitet

  geschätzte 3 % des Gesamtaufkommens

- *Würmer* verbreiten sich über Netzwerke und infizieren alle erreichbaren Systeme

  Wir unterscheiden in User-Interaktions- und Prozessinteraktions

  Basierenden Würmer. (Doppel-Klick-Viren versus Exploit-Based)

Angriffsformen von Viren – Replikations-Orientiert

KARUS SOFTWARE

User-Interaktionsbasierend

„Doppelklick“ eMail Viren, Tanatos, NetSky, Bagle, Sobig.F etc.....setzen Aktion des User´s voraus

Prozess-Interaktionsbasierend

„Klassischer Wurm“ Ein Start ist ausreichend Moris CodeRed Slammer Blaster,

Direct User-involvment Attack

User deaktiviert Sicherung/Hemmnis „Britney-Spears“–Wurm, IRC-Bots,

Indirect User-involvment Attack

User wird via eMail auf Seite gelockt wo erst die eigentliche Attacke passiert Baqle-Q (Carrier eMail) transportiert nur den Link

Exploit-Based Attack

Blaster, Slammer, Witty Nutzt einen bestehenden Exploit von Systemen

Regular Service Based Attack

Jede Form von DDOS wo das Ziel auf Grund „regulärer“ Request versenkt wird. Mydoom.A-F, Bagle.M

Mischformen

zB: URL-Redirection Attack Spam-Mails, Fishing,....

Mischformen

NIMDA, BAGLE.Q, Netsky.P, Sowohl User als auch Prozess basierte Replikation Sowohl Exploit als auch Regular Service

Trojaner/Backdoors sind Programme mit versteckter (schädlicher) Zweitfunktion

Streng genommen zählen Sie, ebenso wie Backdoors NICHT zu den Viren, da sie selbst über keine Replikationsmechanismen verfügen. Der potentiellen Angreifer kann defakto “alles” was auch der User des betroffenen Systems kann.

Bot – Bot-Netze

Als Bot´s werden “Viren” welche eine Kombination aus Backdoor und Wurm beinhalten von potentiellen Angreifern “übernommen” und “kontrolliert”. Die Kommunikation zwischen MasterConsole und Bot erfolgt zumeist über IRC-Netzwerke (Internet Relay Chat)

Adware, Spyware, Dialer, …

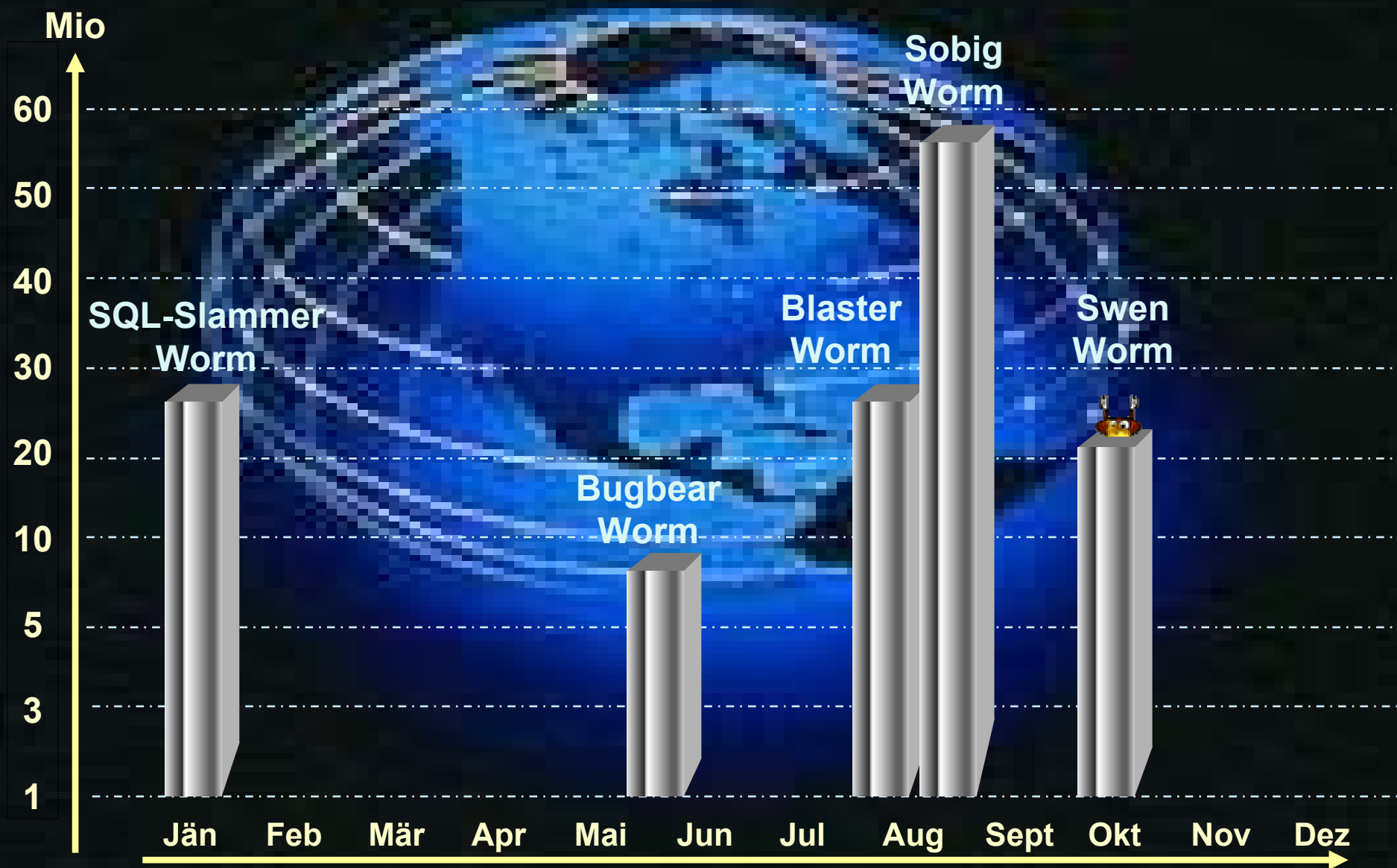
- **Signaturdatenbanken von Virenscannern wachsen “unangenehm” schnell:**
  - Es gibt heute ca. 125.000 verschiedene Schadprogramme (inklusiver vieler „Altlasten“ aus MS DOS-Zeiten)
  - Typisches Wachstumsbeispiel (Trend Micro):
    - August 2001: 4,0 MB
    - Januar 2004: 7,5 MB
    - Januar 2005: 11,8 MB
    - April 2005: 14,7 MB
  - 10 Jahre hat es gebraucht (1991 bis 2001), damit die Datenbank 4 MB groß wird, aber nur wenige Monate, bis sich ihre Größe mehr als verdoppelt und verdreifacht hat
  - Allein in den letzten 4 Monaten ganze 3 MB Wachstum

Quelle: Andreas Marx/Universität Magdeburg

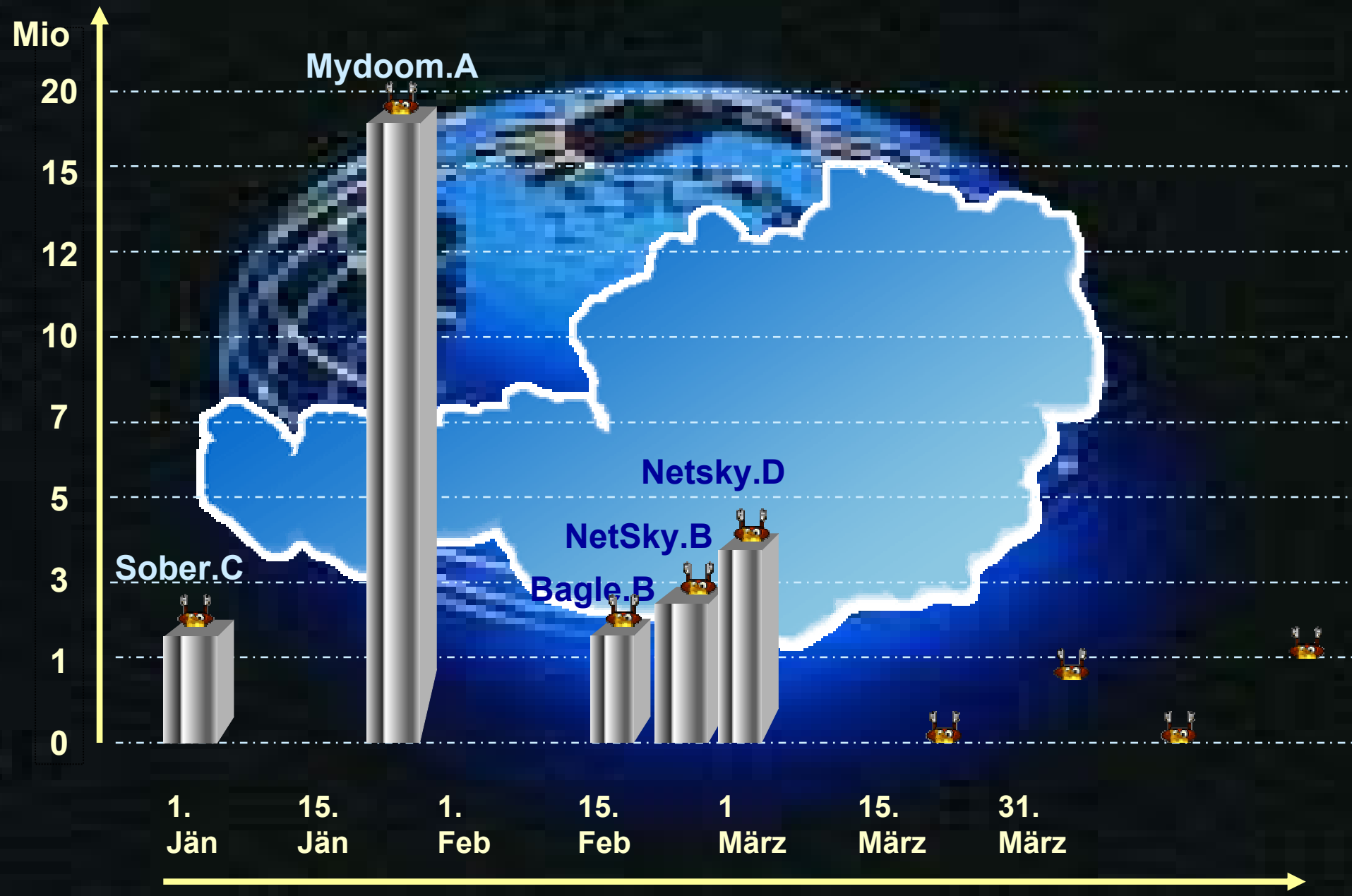
5 Major Outbreaks 2003

KARUS SOFTWARE

Year of the Worm - Anzahl bekannter Viren erreicht über 90 000



5 Major Outbreaks Q1/2004 - Österreich



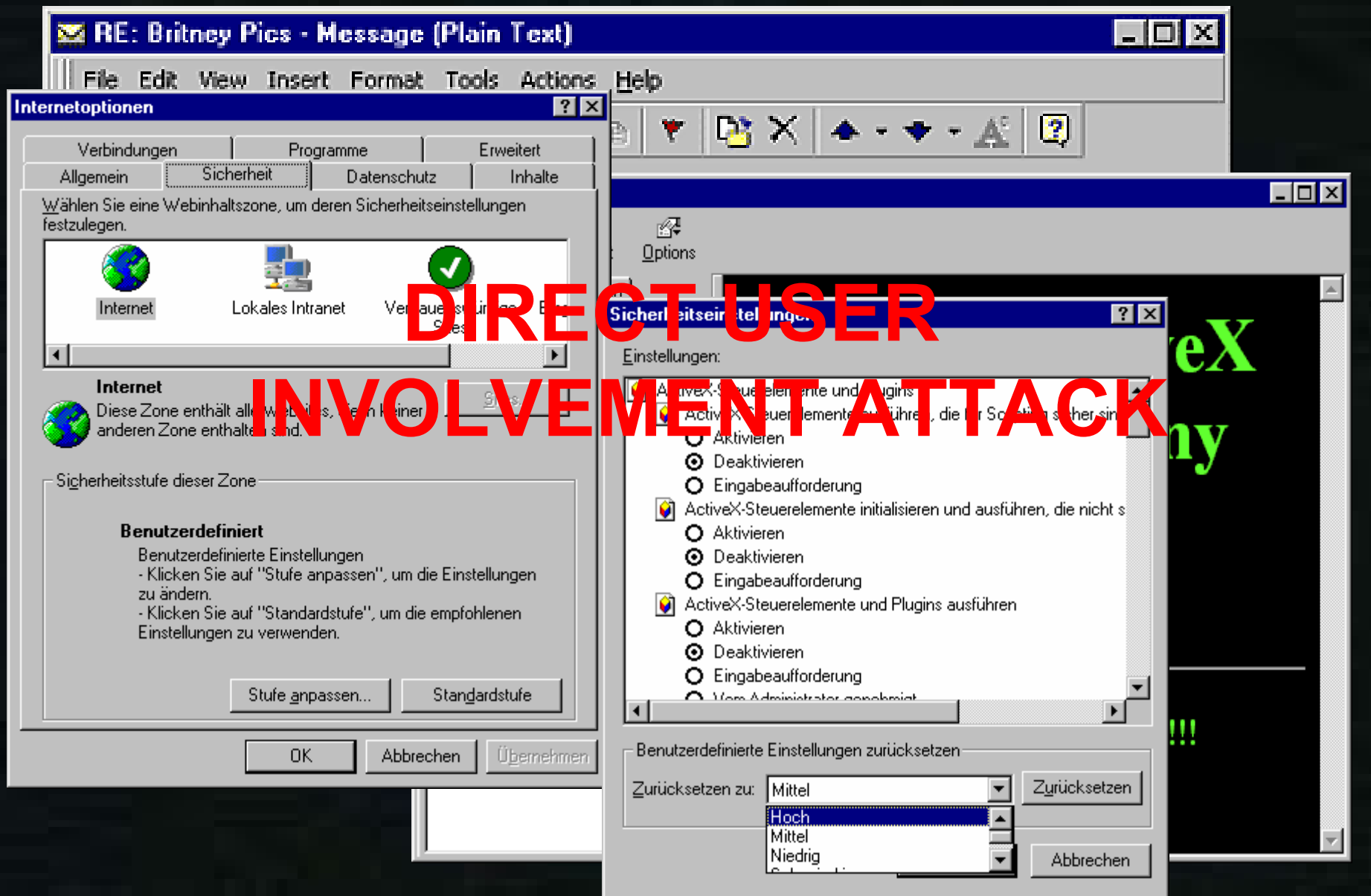
Quo vadis ?

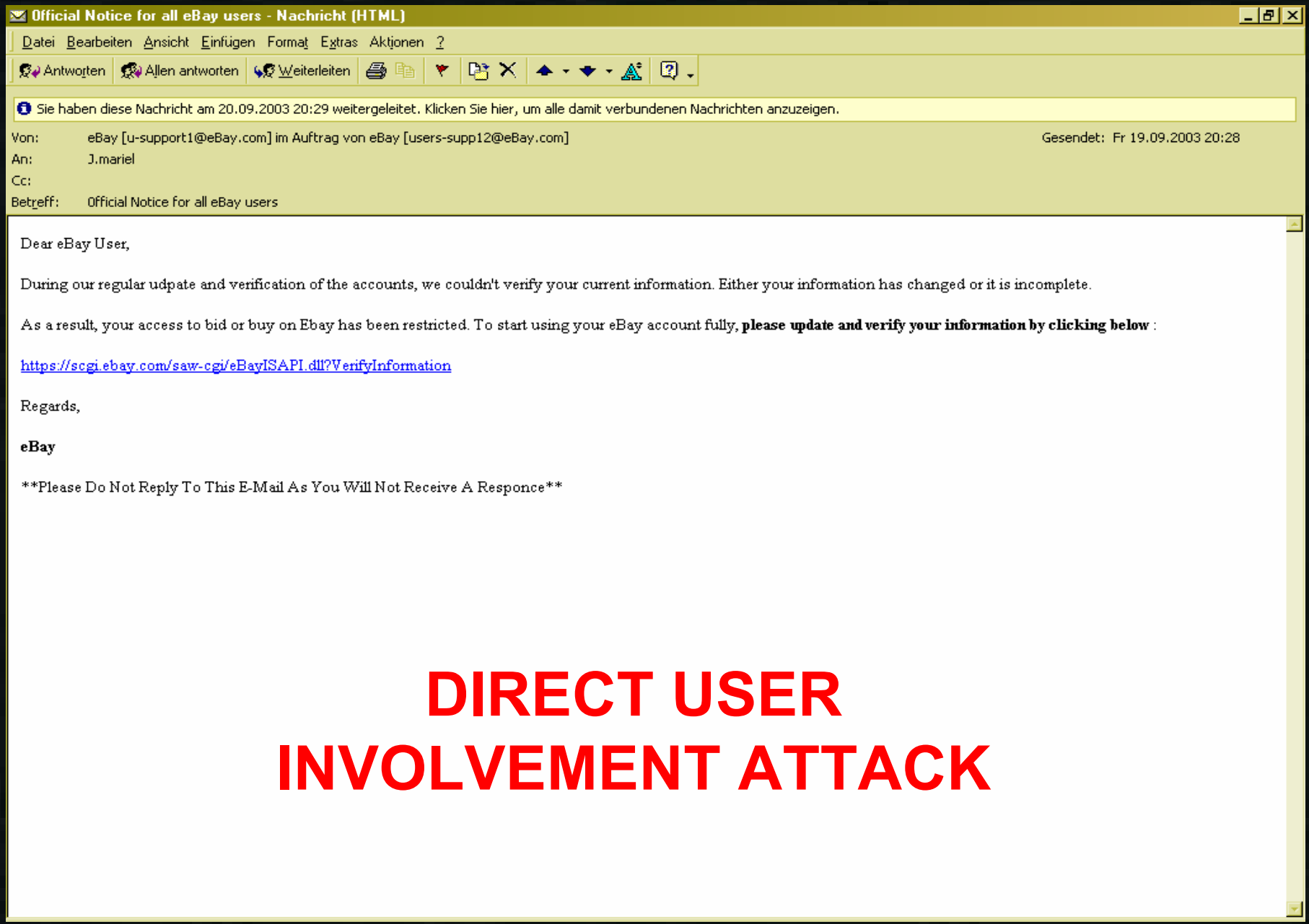
2004 bescherte uns eine Reihe an durchaus „verzichtbaren“ neuen Rekorden.
Die Zahl der eindeutig als Viren indentifizierten Programme durchbrach von 1986 an gerechnet das erste Mal die 100.000er Marke, und brachte zudem einen neuen „Monatsrekord“ mit über 1.800 neuen Viren/Malicious Codes im Spitzenmonat März.
Je nach Spammer-Aktivität werden zwischen 62% und 74% aller erhaltenen Emails in Österreich als Spam-Mails klassifiziert. Im Spitzenfeld liegen dabei Unternehmen mit über 200.000 erhaltenen Spam-Mails pro Tag. Diese Werte schwemmen Tag für Tag konstant „Müll“ in die User-Mailboxen. Im Vergleich dazu liegt das Viren-Aufkommen bei 14-16% an „ruhigen“ Tagen. An Tagen mit High-Outbreak-Phasen verschiebt sich die Relation „infiziertes eMail“ versus „virenfreies eMail“ kurzfristig mit Spitzen bis zum Verhältnis 1:7 (nur mehr jedes 7 Mail ist ein Viren-Freies eMail). Etwa beim Sober.F oder im Verhältnis 1:4,5 beim Sobig.I !

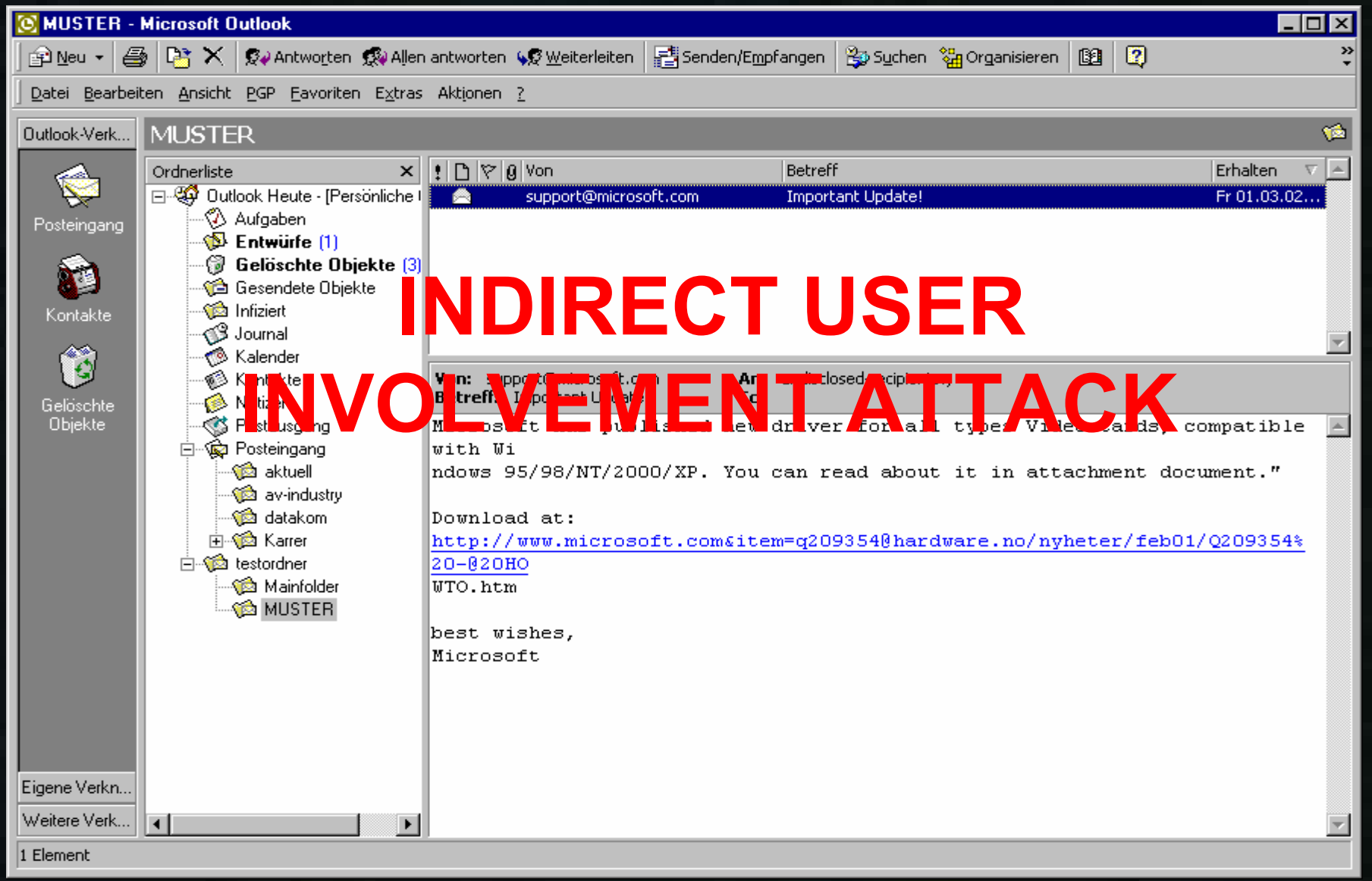
Trojan - Generator

Trojanerschreiben für Dummies




RE: Britney Pics - Message (Plain Text)
File Edit View Insert Format Tools Actions Help
Internetoptionen
Verbindungen
Programme
Erweitert
Allgemein
Sicherheit
Datenschutz
Inhalte
Wählen Sie eine Webinhaltszone, um deren Sicherheitseinstellungen festzulegen.
Internet
Lokales Intranet
Internet
Sicherheitsstufe dieser Zone
Benutzerdefiniert
Benutzerdefinierte Einstellungen
- Klicken Sie auf "Stufe anpassen", um die Einstellungen zu ändern.
- Klicken Sie auf "Standardstufe", um die empfohlenen Einstellungen zu verwenden.
Stufe anpassen...
Standardstufe
OK
Abbrechen
Übernehmen
Options
Einstellungen:
Aktivieren
Deaktivieren
Eingabeaufforderung
ActiveX-Steuerelemente initialisieren und ausführen, die nicht s
Aktivieren
Deaktivieren
Eingabeaufforderung
ActiveX-Steuerelemente und Plugins ausführen
Aktivieren
Deaktivieren
Eingabeaufforderung
Benutzerdefinierte Einstellungen zurücksetzen
Zurücksetzen zu:
Mittel
Zurücksetzen
Hoch
Mittel
Niedrig
Abbrechen
DIRECT USER
INVOLVEMENT ATTACK


Official Notice for all eBay users - Nachricht (HTML)
Datei Bearbeiten Ansicht Einfügen Format Extras Aktionen ?
Antworten Allen antworten Weiterleiten
Sie haben diese Nachricht am 20.09.2003 20:29 weitergeleitet. Klicken Sie hier, um alle damit verbundenen Nachrichten anzuzeigen.
Von: eBay [u-support1@eBay.com] im Auftrag von eBay [users-supp12@eBay.com]
Gesendet: Fr 19.09.2003 20:28
An: J.mariel
Cc:
Betreff: Official Notice for all eBay users
Dear eBay User,
During our regular udpate and verification of the accounts, we couldn't verify your current information. Either your information has changed or it is incomplete.
As a result, your access to bid or buy on Ebay has been restricted. To start using your eBay account fully, please update and verify your information by clicking below :
https://scgi.ebay.com/saw-cgi/eBayISAPI.dll?VerifyInformation
Regards,
eBay
Please Do Not Reply To This E-Mail As You Will Not Receive A Responce
DIRECT USER
INVOLVEMENT ATTACK



INDIRECT USER INVOLVEMENT ATTACK

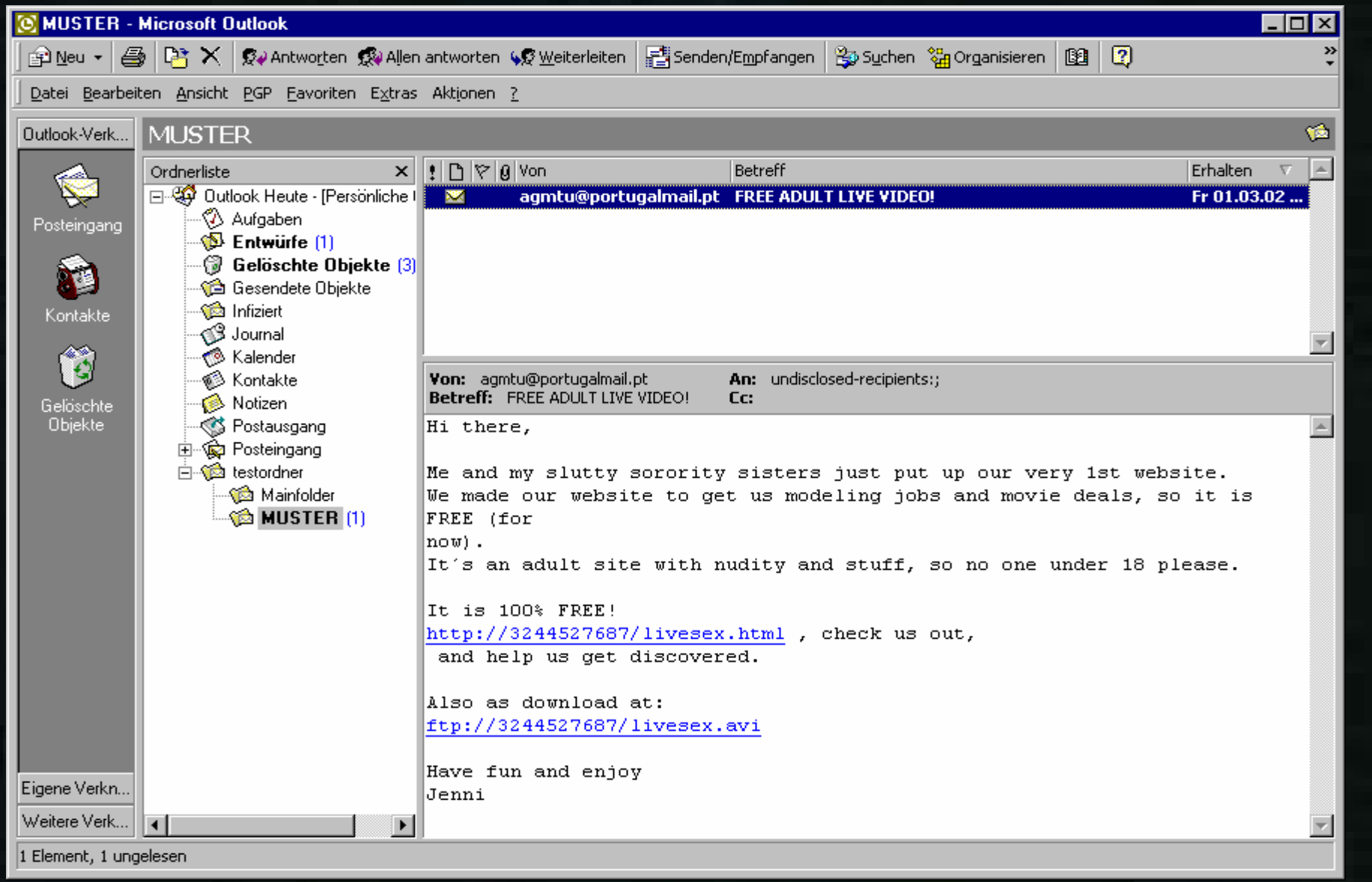
URL-Redirection Attack

http://www.microsoft.com&item=q209354@hardware.no/nyheter/feb01/Q209354%20-@20HOWTO.htm

Url Redirection using the @ Symbol

Url Redirection using DNS spoofing

Url Redirection using DNS cache injection


MUSTER - Microsoft Outlook
Neu
Antworten
Allen antworten
Weiterleiten
Senden/Empfangen
Suchen
Organisieren
Datei Bearbeiten Ansicht PGP Favoriten Extras Aktionen ?
Outlook-Verk...
MUSTER
Posteingang
Kontakte
Gelöschte Objekte
Ordnerliste
Outlook Heute - [Persönliche
Aufgaben
Entwürfe (1)
Gelöschte Objekte (3)
Gesendete Objekte
Infiziert
Journal
Kalender
Kontakte
Notizen
Postausgang
Posteingang
testordner
Mainfolder
MUSTER (1)
Von
Betreff
Erhalten
agmtu@portugalmail.pt FREE ADULT LIVE VIDEO! Fr 01.03.02 ...
Von: agmtu@portugalmail.pt
An: undisclosed-recipients:;
Betreff: FREE ADULT LIVE VIDEO!
Cc:
Hi there,
Me and my slutty sorority sisters just put up our very 1st website.
We made our website to get us modeling jobs and movie deals, so it is
FREE (for
now).
It´s an adult site with nudity and stuff, so no one under 18 please.
It is 100% FREE!
http://3244527687/livesex.html , check us out,
and help us get discovered.
Also as download at:
ftp://3244527687/livesex.avi
Have fun and enjoy
Jenni
Eigene Verkn...
Weitere Verk...
1 Element, 1 ungelesen

„undotted“ IP Adress Attack

IE Trusted Sites can be facked

http://3244527687/livesex.html

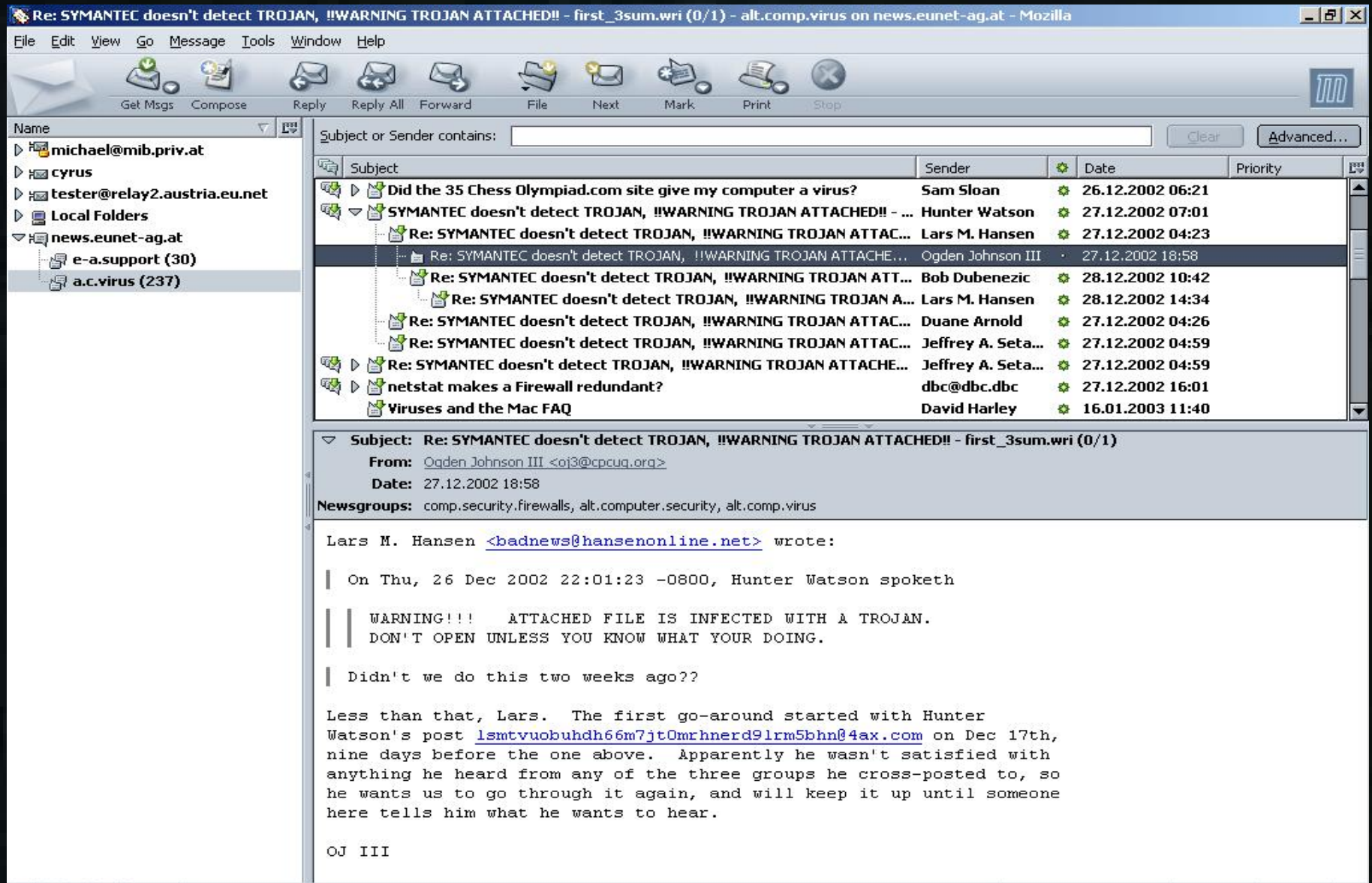
Using „undotted“ IP Adresses (e.g. 3244527687 = 193.99.144.71)

► „undotted“ IP Adresses override „IE Trusted Site Settings“

► Local Security restrictions apply – insecure web surfing

Newsgroups verbreiten Viren

KARUS SOFTWARE



Bearbeiten Ansicht Favoriten Extras ?
Zurück Suchen Favoriten Medien
http://www.heise.de/newsticker/meldung/57030
Wechseln zu

heise online

Bewerber-Datenbank für Ingenieure.
www.ingenieurkarriere.de

che ...
age-News
ws-Archiv
ws mobil
wsletter
ws einbinden
efontarife
rnettarife
rnetstörungen
erforum
at-Events
glish Pages
o & Heft
ntakt
diadaten
ECHNOLOGY
empfehlen
LINE-MARKT
Werbung
isvergleich
herchieren und
gleichen in über

news 03.03.2005 14:32

<< Vorige | Nächste >>

Pädophilieverdacht durch infizierten Computer

Als Folge eines heimlich eingeschleusten Programms in seinem Computer hat der schwedische Jurist Magnus Eriksson fünf Jahre unschuldig mit dem Vorwurf der Pädophilie leben müssen. Wie der 41-Jährige am Donnerstag im schwedischen Rundfunksender SR bestätigte, hatte er 1999 seinen Forschungsjob an der Universität Lund verloren, nachdem in seinem Arbeitscomputer 12.000 pornografische Bilder, davon 3.000 mit Kindern, entdeckt worden waren. Das erst Ende vergangenen Jahres eingeleitete Gerichtsverfahren brachte in allen Punkten einen Freispruch, weil eindeutig erwiesen war, dass jemand anders die Pornobilder mit Hilfe eines auf dem PC installierten Trojaners heruntergeladen hatte.

Die Leitung der Juristischen Fakultät hatte sofort nach Bekanntwerden des Verdachtes Erikssons Namen an das Personal der Uni weitergegeben und dem Betroffenen Hausverbot erteilt. Der Jurist berichtete im Rundfunk, er sei danach auf der Straße von Studenten beschimpft und verspottet worden. Mit seiner Frau zog er deshalb nach Spanien um, wo er weiter krank und ohne Arbeit lebt.

Bis zur Erhebung einer Anklage vergingen zwei und bis zur Urteilsfindung weitere drei Jahre. Erst zum Prozess erhielten technische Experten der Verteidigung Zugang zu dem PC und konnten nachweisen, dass dort eine von einem Schweden geschriebene Software zur unbemerkten Steuerung des Rechners von außen installiert war. Es erwies sich zudem, dass die Pornobilder auf Erikssons Computer überhaupt nicht geöffnet und angeschaut worden waren.

Eriksson sagte zu seinem Freispruch, dass ihm auch dieser nach aller Erfahrung in der juristischen Branche nicht beim Wiederaufbau der zerstörten Berufskarriere helfen werde: "Der Makel des Kinderschänders ist das Schlimmste, was man in unserer Gesellschaft angehängt bekommen kann. Er bleibt hängen." Ein Polizeisprecher bedauerte, dass die eigenen Experten das unsichtbare PC-Programm nicht hatten finden können. (*dpa*) / (dab/c't)

News suchen
los!
Hilfe

Top-Meldungen
Knoppix 3.8 kommt zur CeBIT
Softwarepatente: Das riskante Spiel der EU-Kommission
FOSDEM: Open Source und die Rückkehr zum Einfachen
Free Software Foundation Europe startet Fellowship-Programm

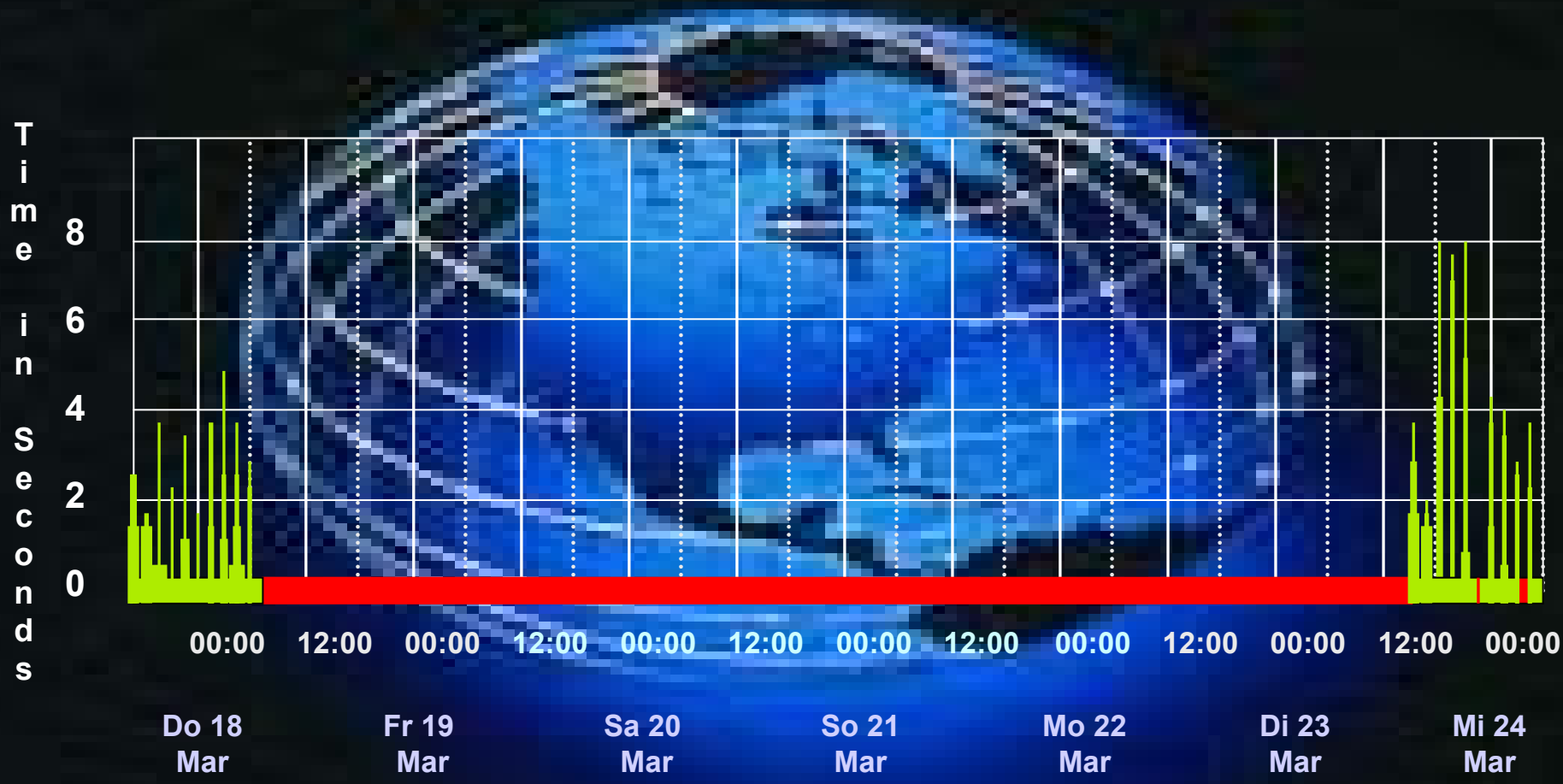
Aktuelle Meldungen
Pädophilieverdacht durch infizierten Computer
IG Metall will Schließung des Münchner Infineon-Werks verhindern
CeBIT Bahn und T-Mobile starten WLAN-Versorgung der ICE-

Konsequenz der MyDoom.F Attacke für RIAA WebServer



Konsequenz der MyDoom.F Attacke für RIAA WebServer

IKARUS SOFTWARE

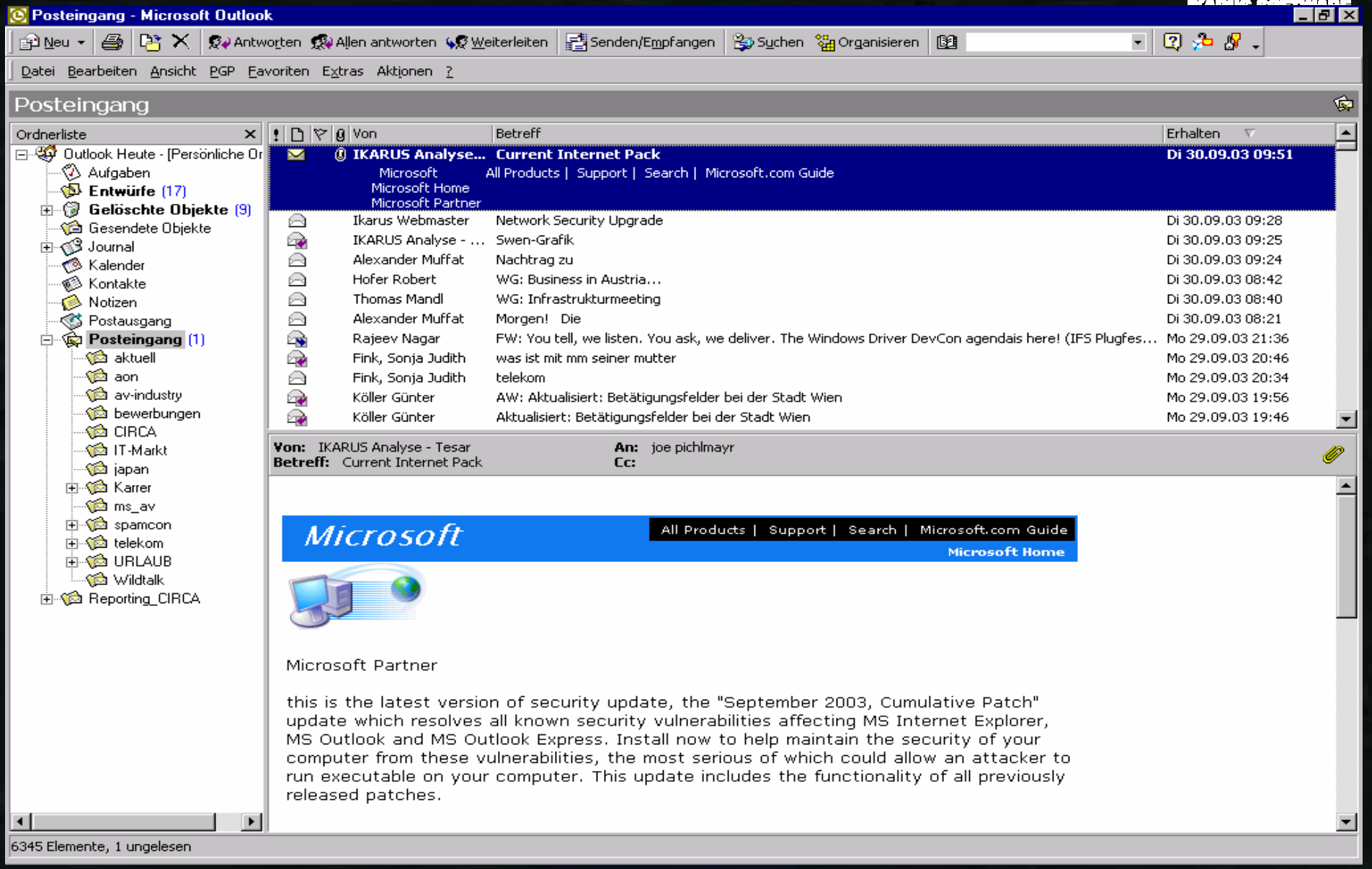


Total time from Amsterdamm/Cee-kay to www.riaa.com

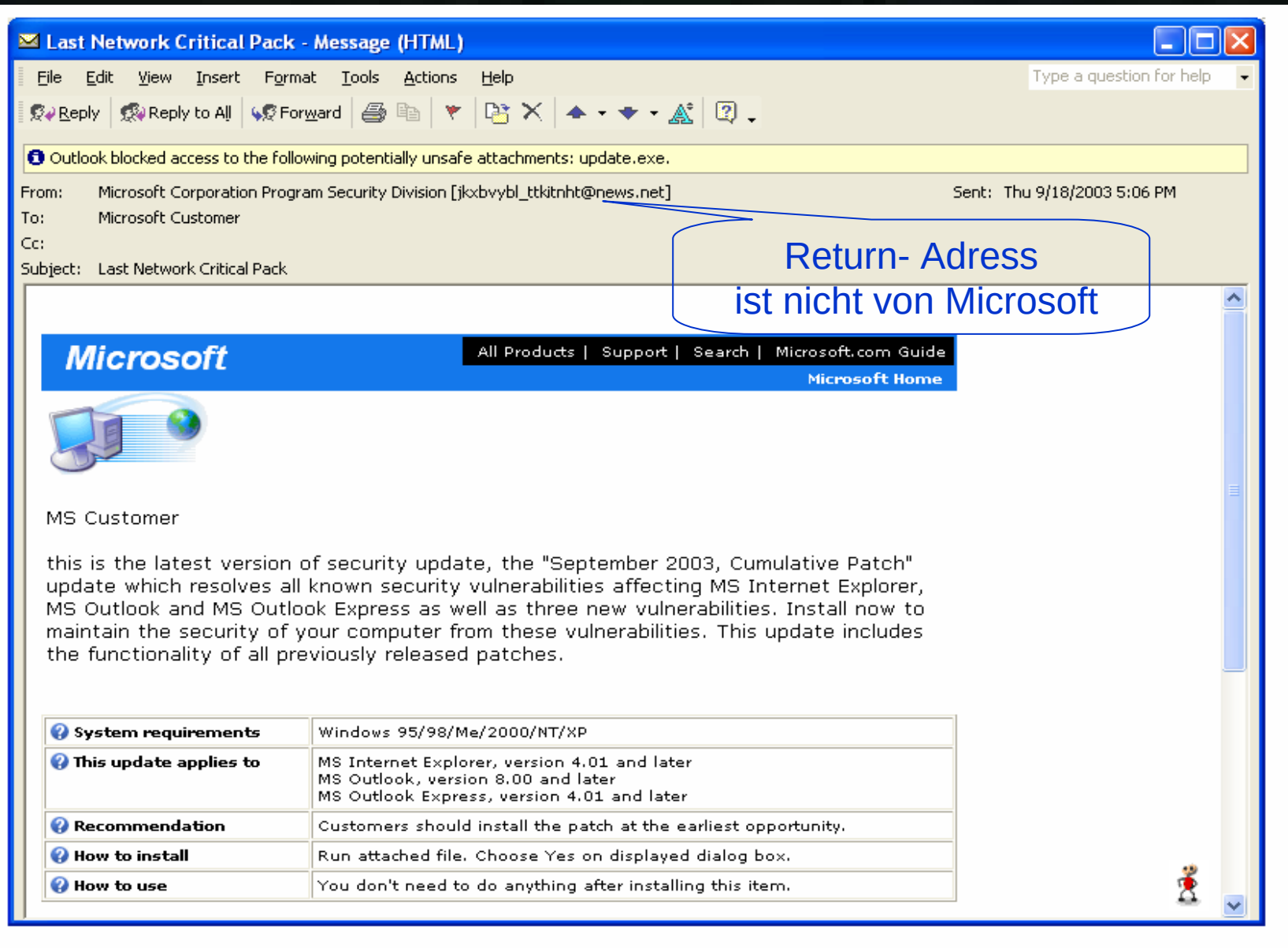
Failures

Quelle: www.netcraft.com

Social Engineering - I.Worm.SWEN.A

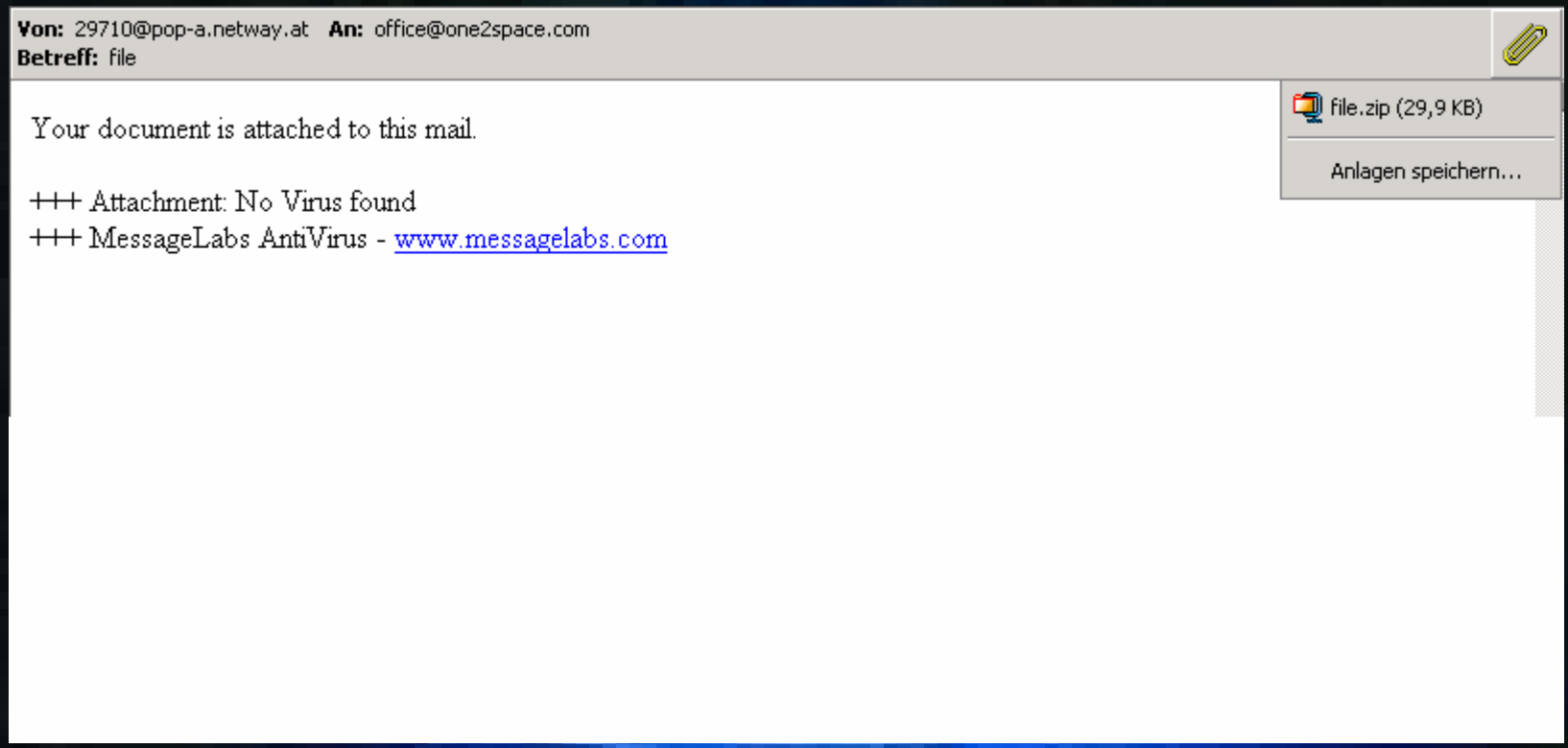


Social Engineering - I.Worm.SWEN.A

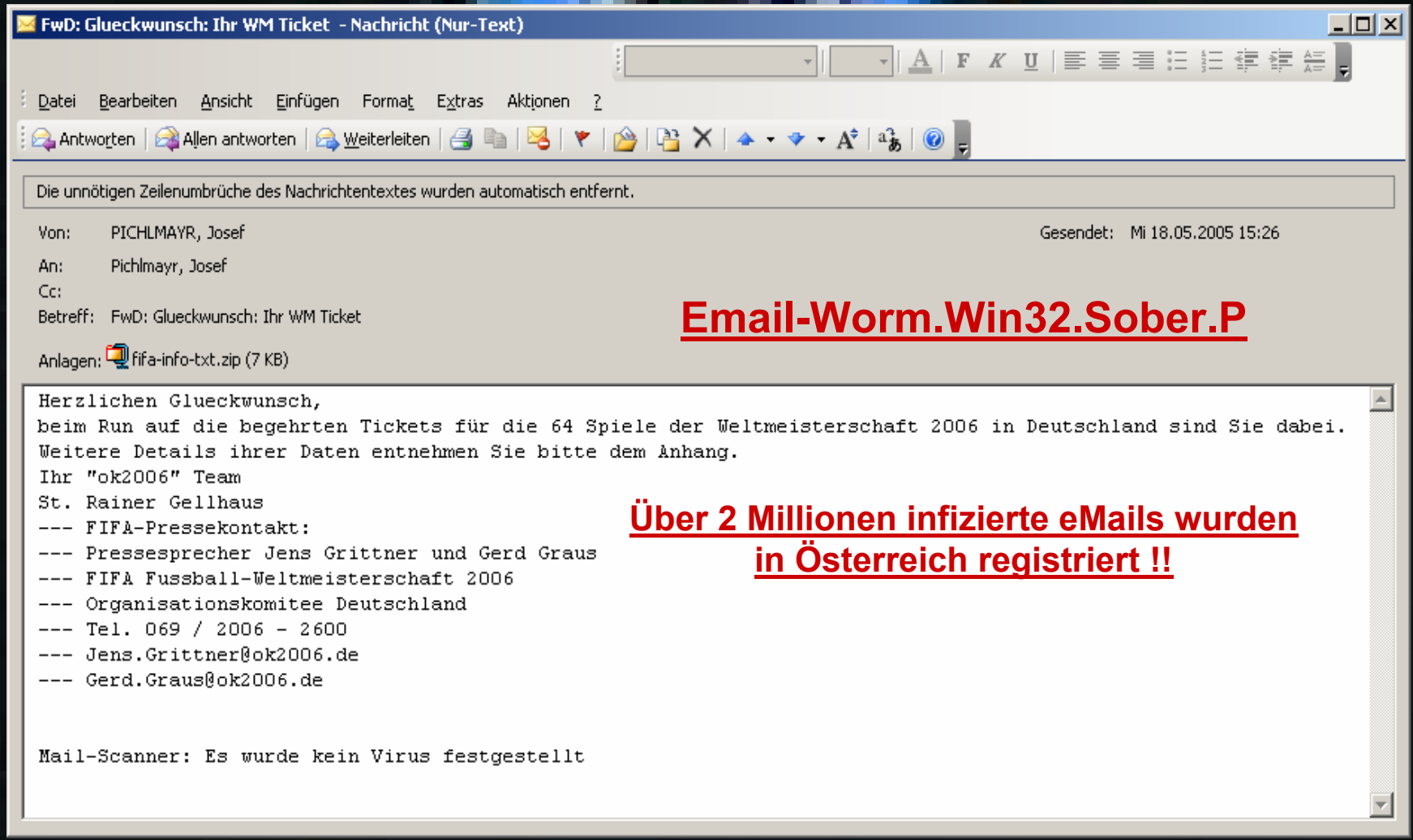


Social Engineering - I.Netsky.P

IKARUS SOFTWARE



aktuell…



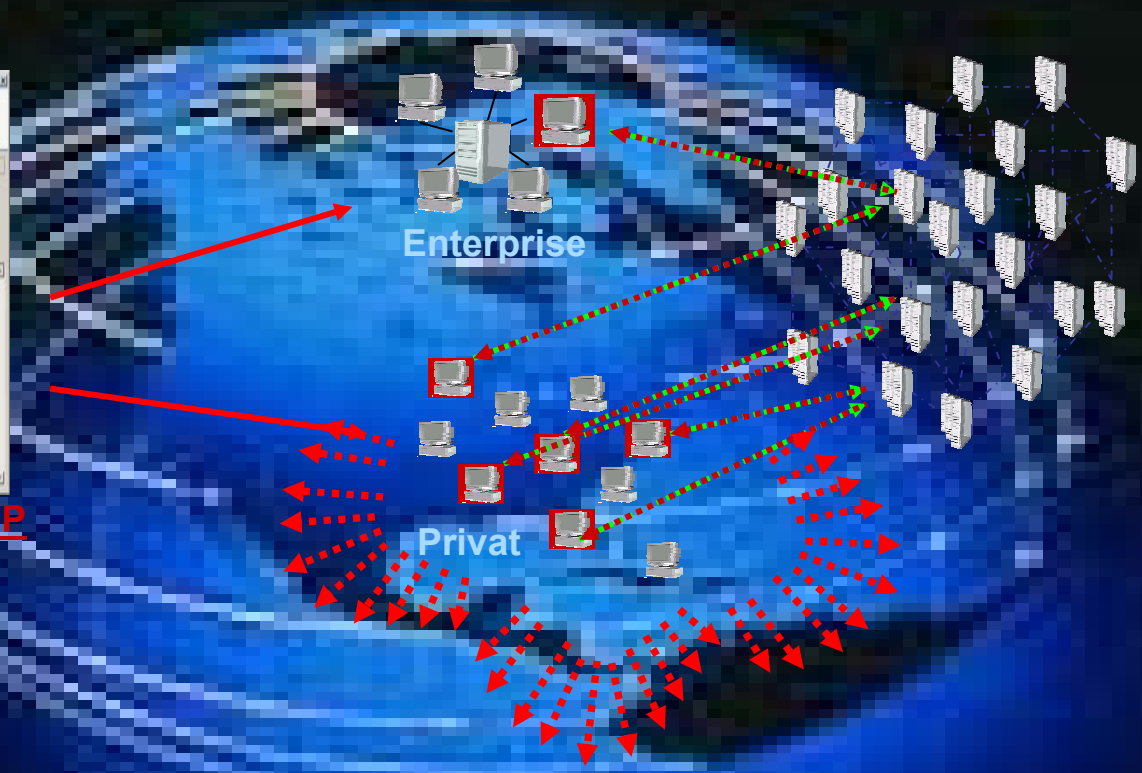
Email-Worm.Win32.Sober.P

Über 2 Millionen infizierte eMails wurden in Österreich registriert !!

Email-Worm.Win32.Sober.Q



Email-Worm.Win32.Sober.P



Kein Virus – Jedoch Mails
Mit rechtsradikalen Inhalten
Tageshöchstwert: 800 000

W32.SQLSlammer.Worm – processinteraction based attack



Initializing Attacker

Buffer Overflow Attack

Targeted system process

corrupted system process

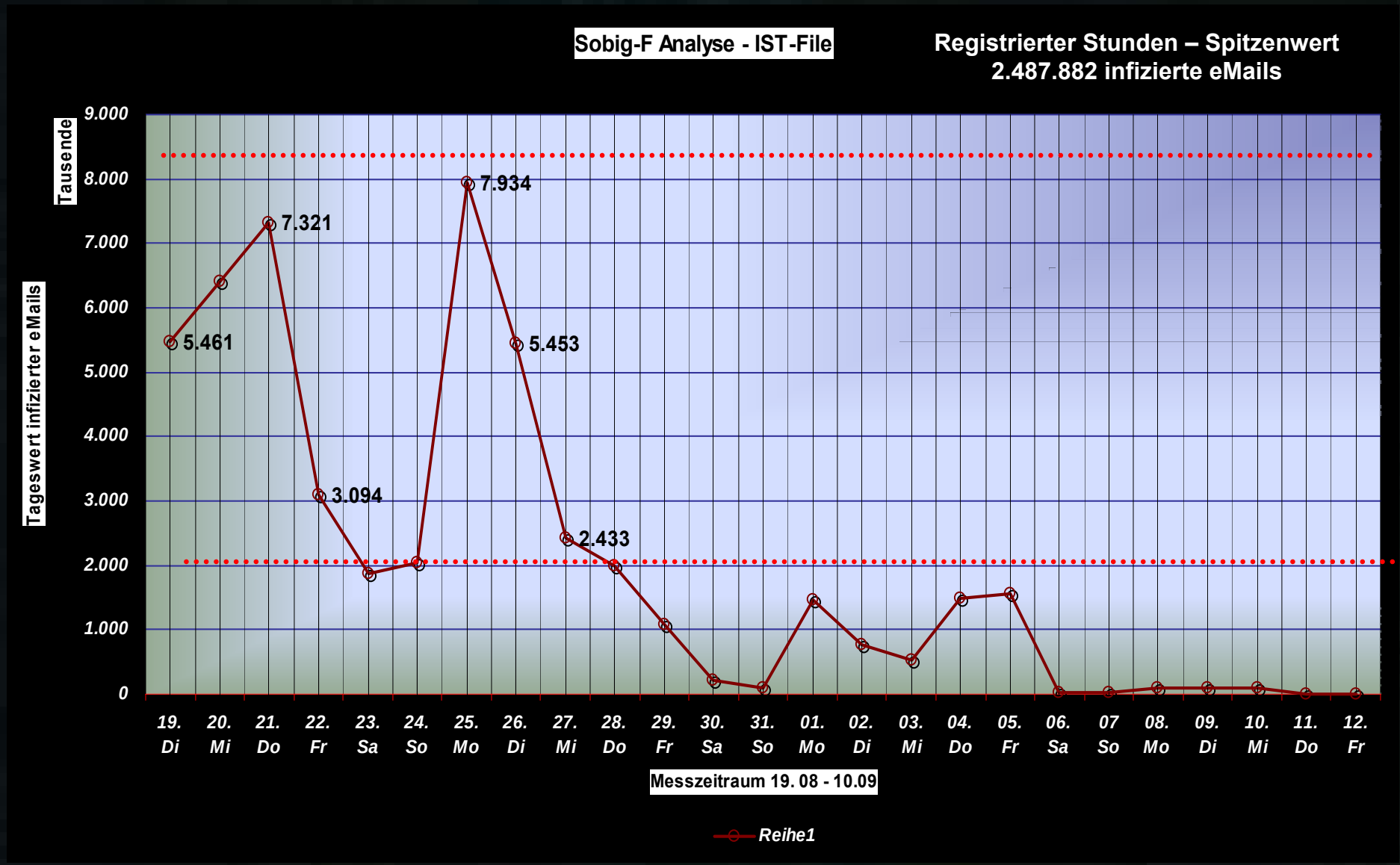
Scan for IP Adresses

192.168.56.45
192.168.56.49
192.168.56.72
192.168.56.91

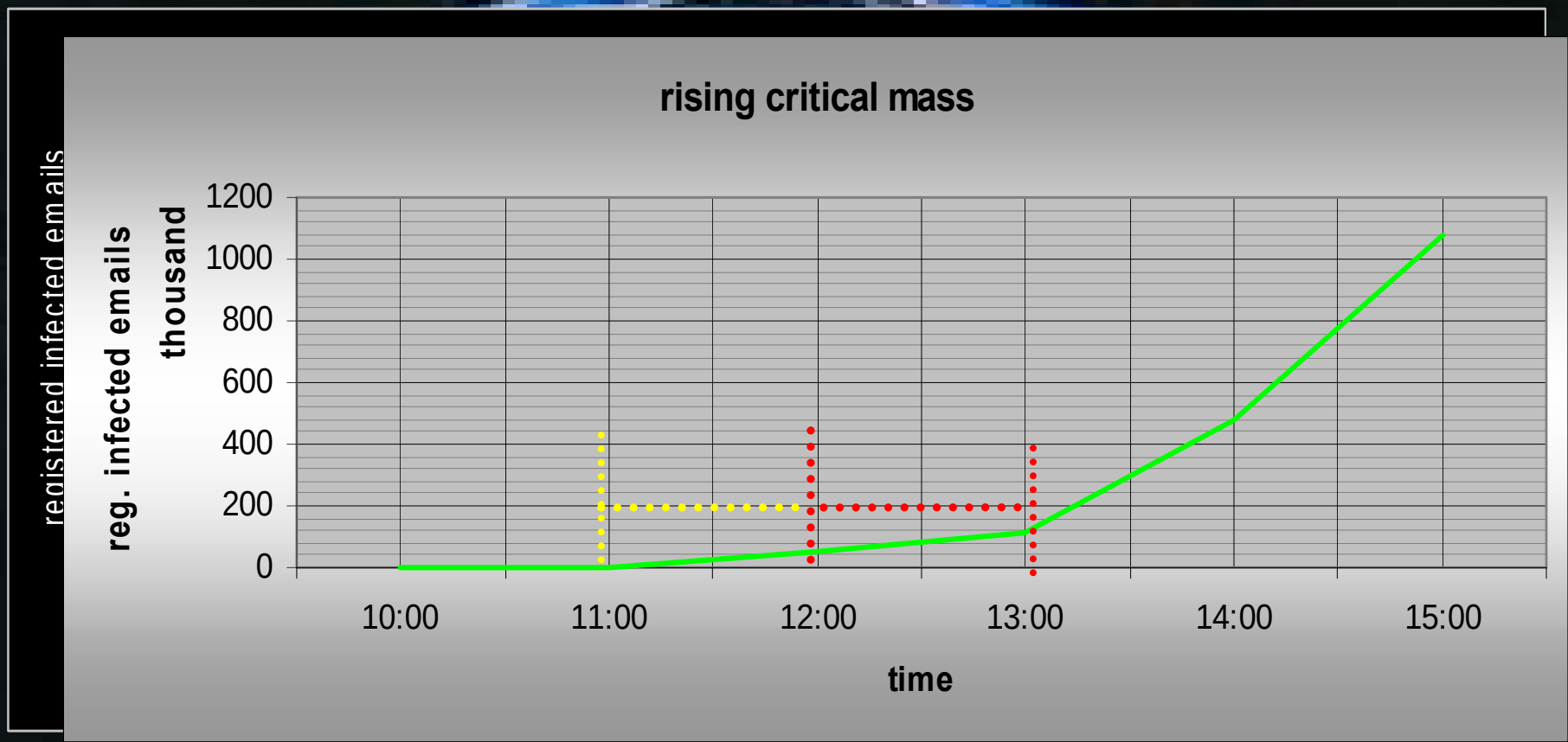
© 2002 IKARUS Software

SOBIG.F

55 Millionen Infizierte eMails in Österreich

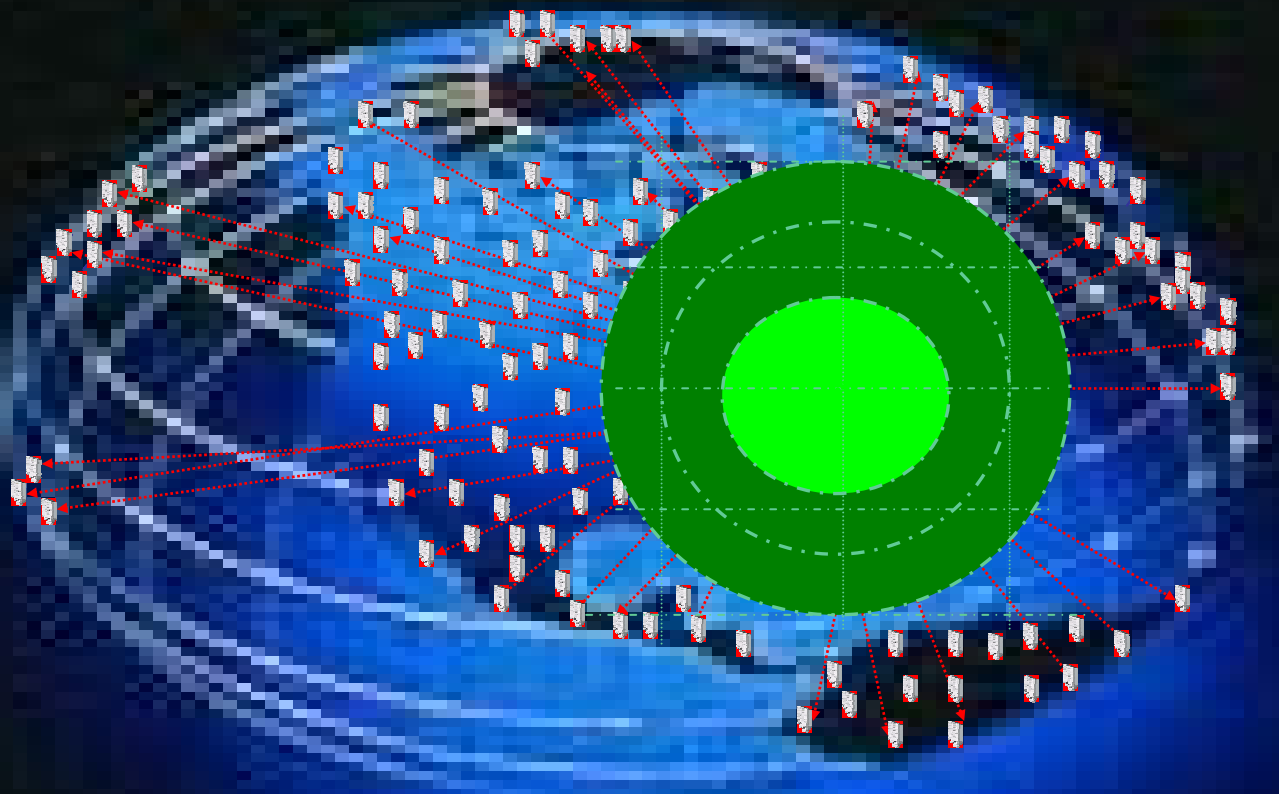


Wesentlicher Response Faktor: Z E I T



C I R C A -Virus Early Warning System

IKARUS SOFTWARE



„Loveletter“ with Early Warning System

IKARUS SOFTWARE

Activity:		Hours:
05:30	„Loveletter“ first sight in Austria	00:00
07:30	Early Warning System allows appraisal of the danger	02:00
07:35	Providers and AV companies are informed	02:05
08:05	First Analyse and Updates from the AV-Companys	02:35
08:05	Specific warning in and about media	02:35
10:00	Point of No Return	04:30

Sensors Early Warning System

Transmission



Logs

From the algorithms / scanner - log files in VIX hosted Ikarus Scan centre . As well as appearing "patterns" in case of virus activity .

1,8 Mio eMails per week

Incident



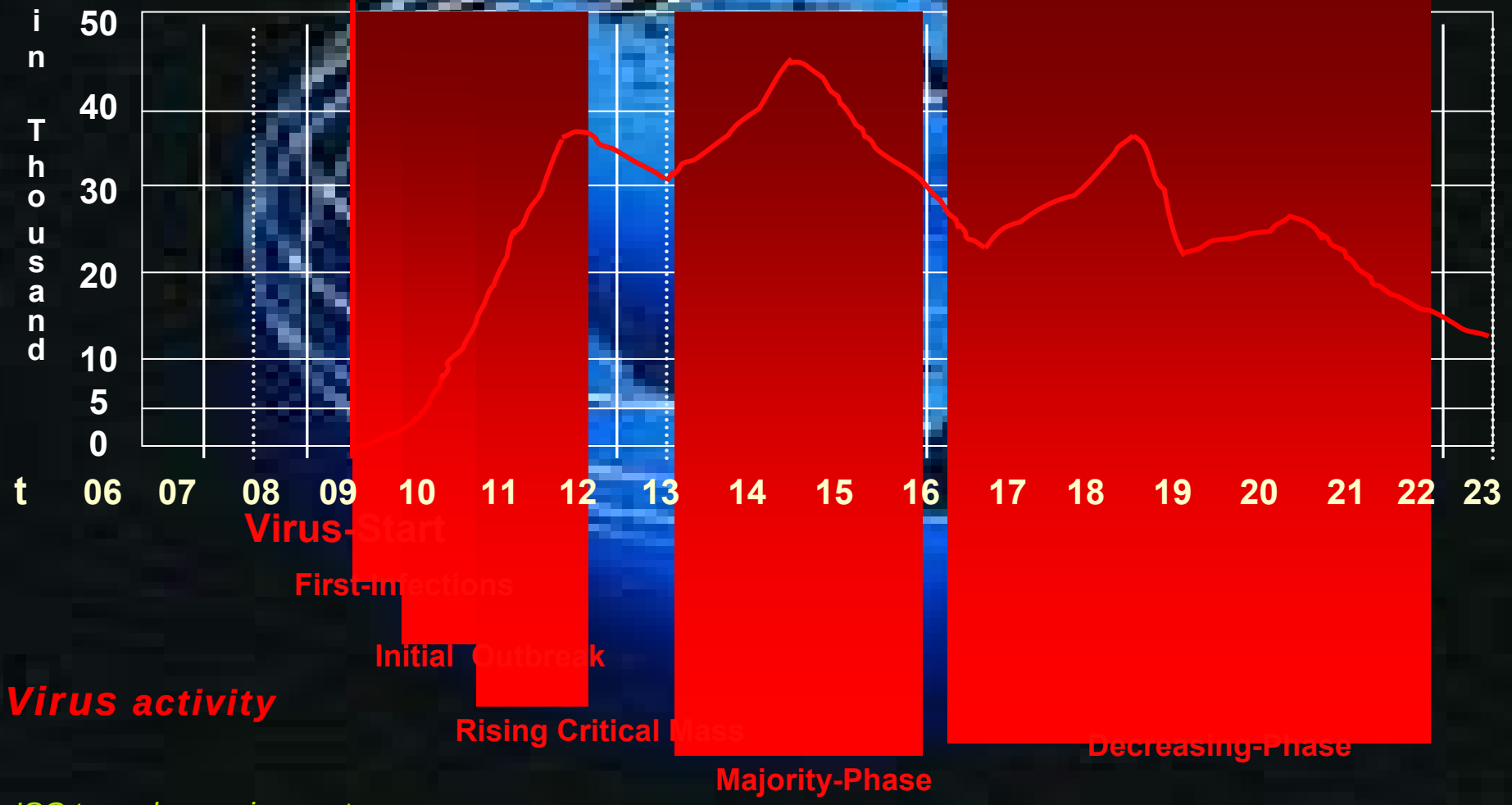
Bait-sample

„Harvest " from Honeypots complementary to the behavior of the log from of the transmission area - Secondary activity .

During "quiet" days about 2,000 Virus/Bots/Spyware per day with an average size of 25-50 kb (about 70 MB per Day)

During "worried" days clearly about a gigabyte!

1st Day - Outbreak-Characteristics
based on Sober-I

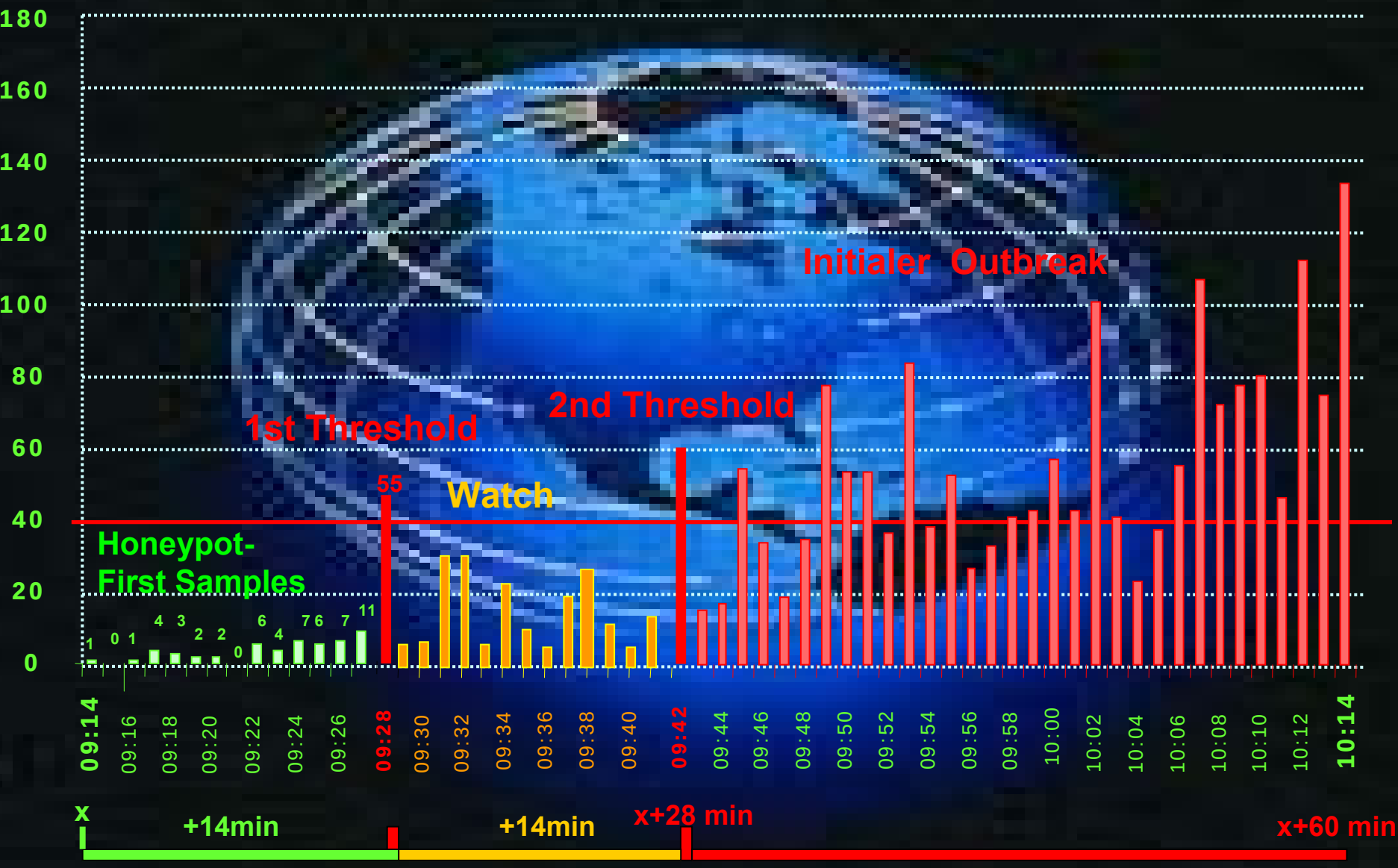


ISC to early warning system

Quelle: www.ikarus.at

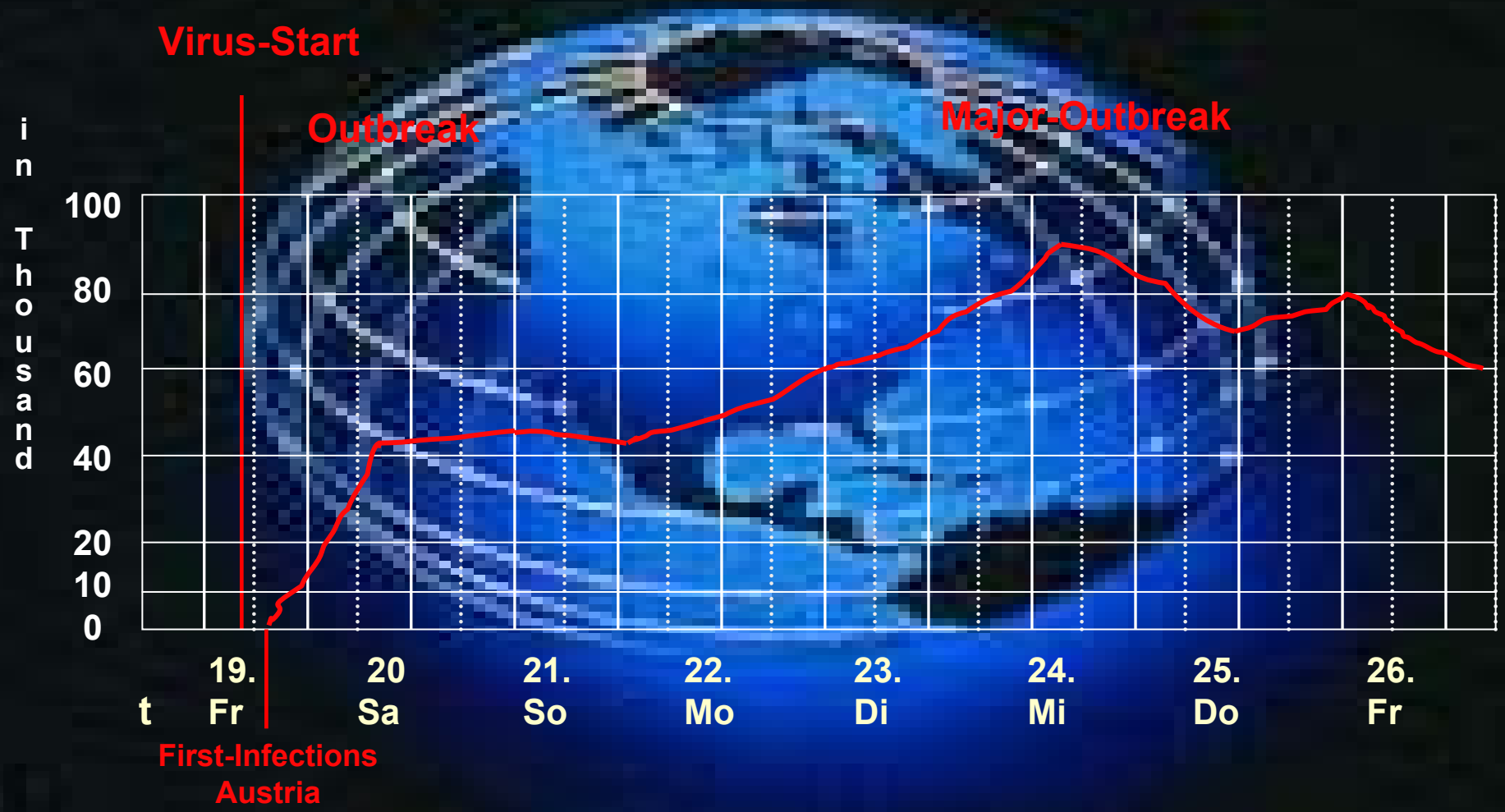
1st HOUR - Outbreak-Characteristics

based on Sober-I



1st Week - Outbreak-Characteristics

based on Sober-I Timeline



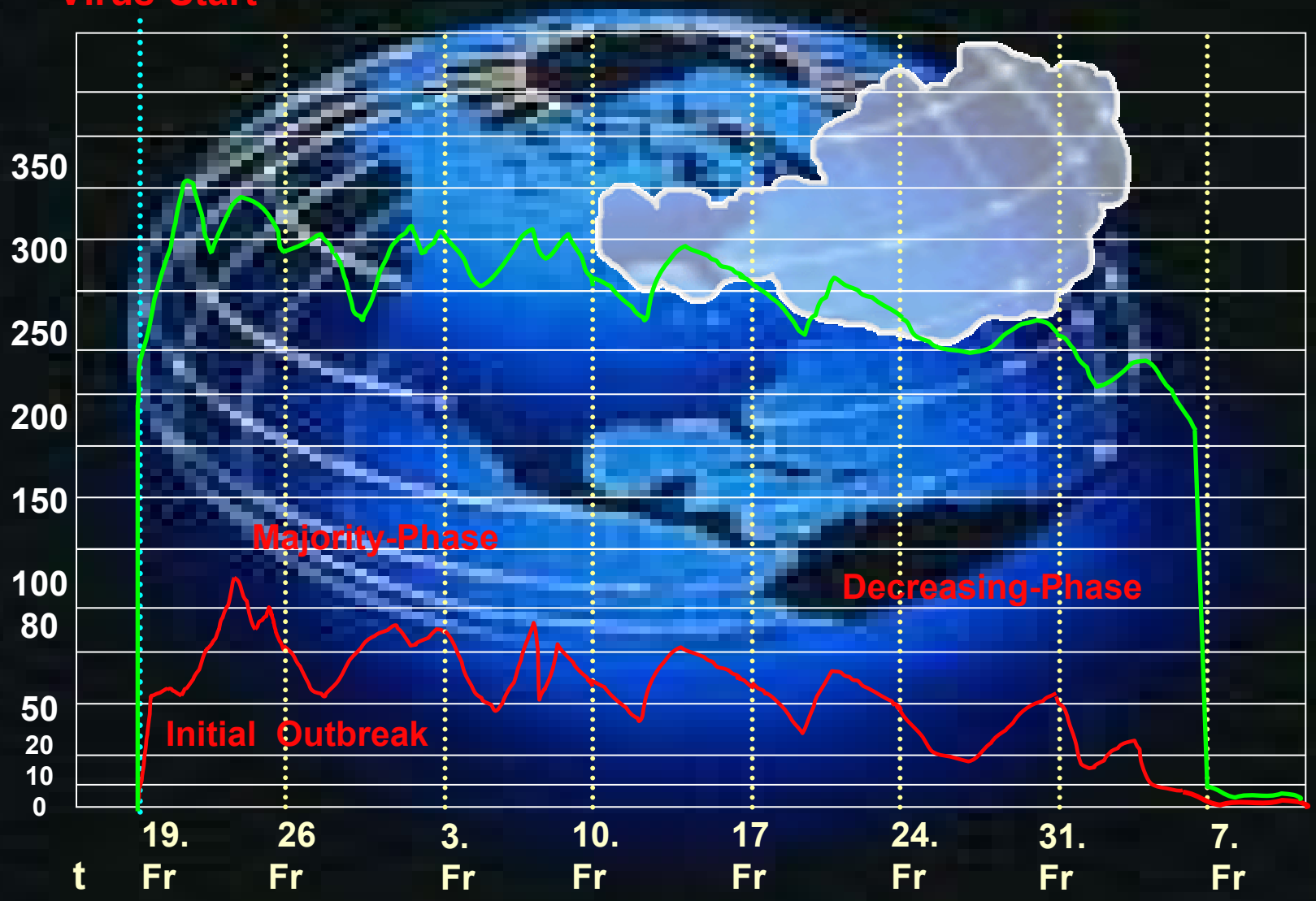
ISC to early warning system

Quelle: www.ikarus.at

Total Period - Outbreak-Characteristics

based on Sober-I 9.11.2004 – 06.01.2005 Timeline

with Telekom Austria Figures

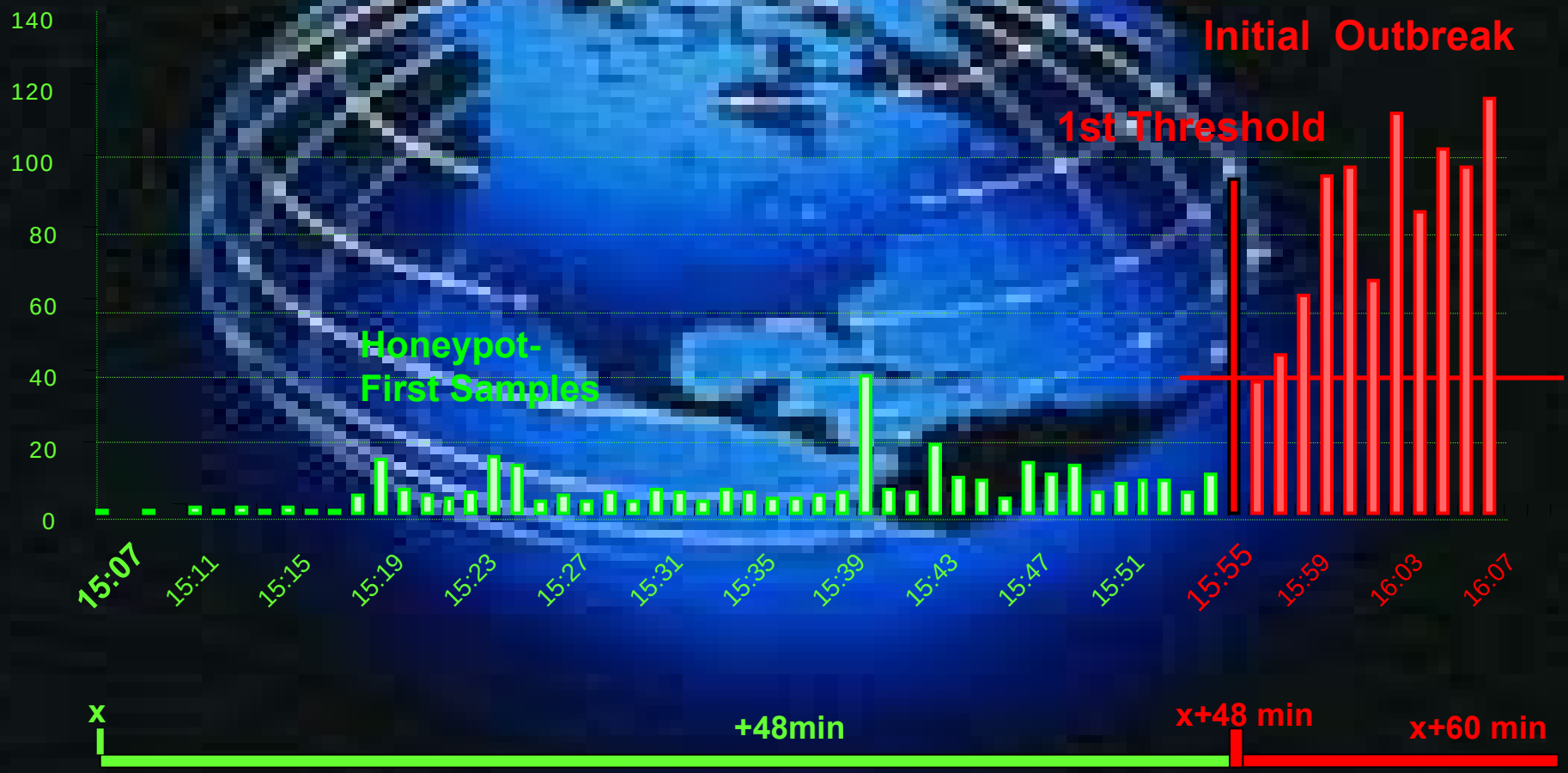


ISC to early warning system

Quelle: Ikarus/Telekom

1st HOUR - Outbreak-Characteristics

based on Zafi.D

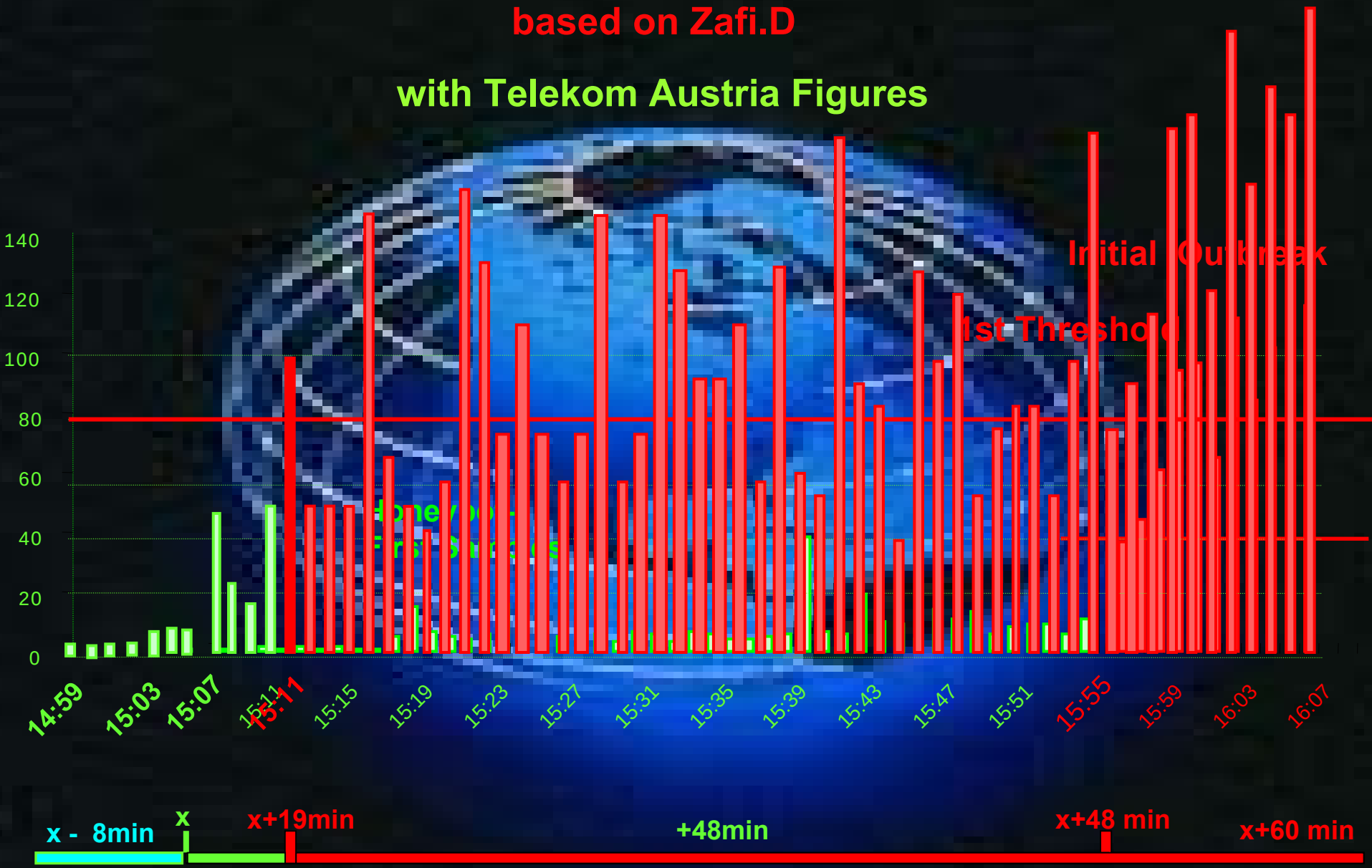


ISC to early warning system

Quelle: www.ikarus.at

1st HOUR - Outbreak-Characteristics based on Zafi.D

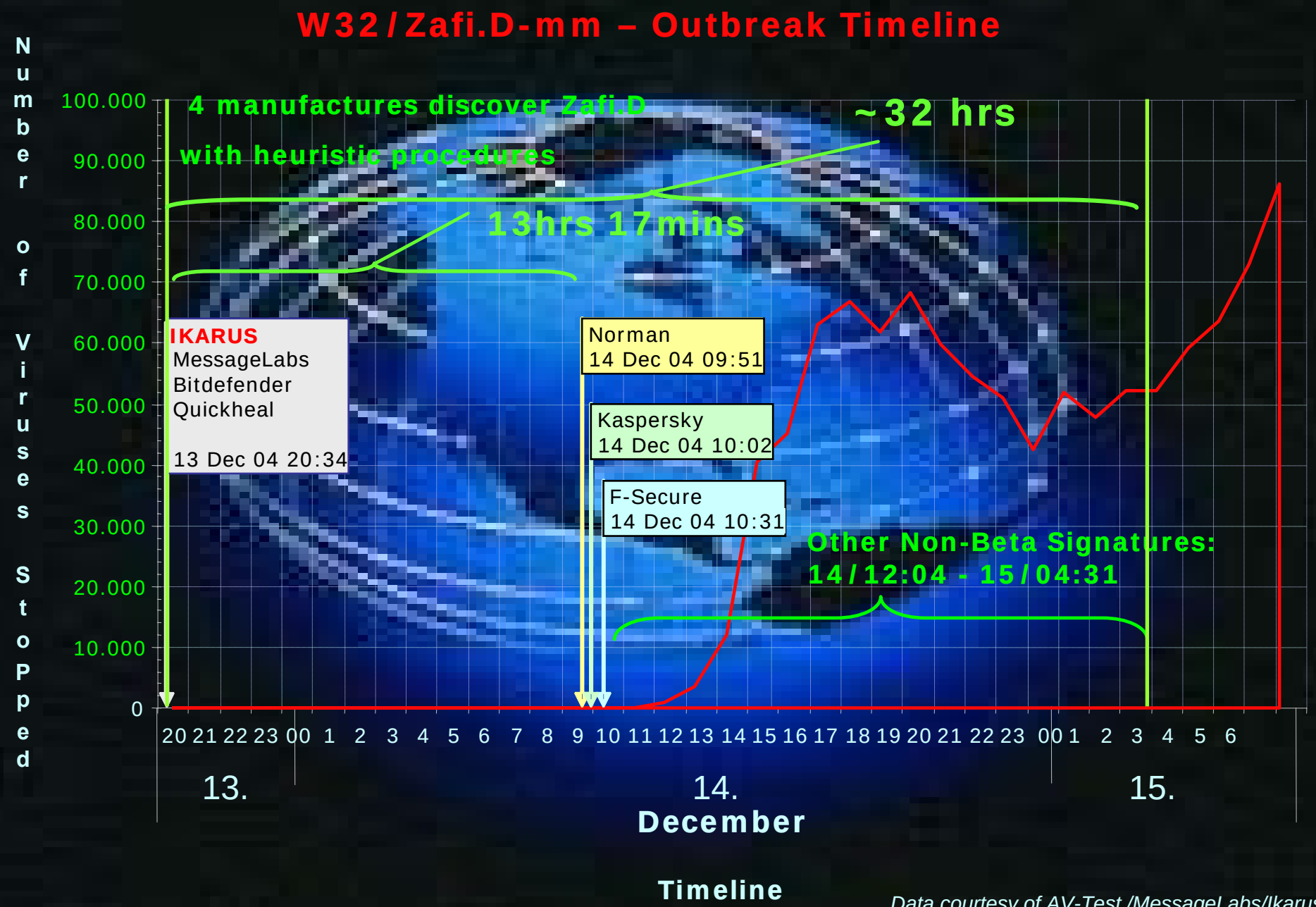
with Telekom Austria Figures



ISC to early warning system

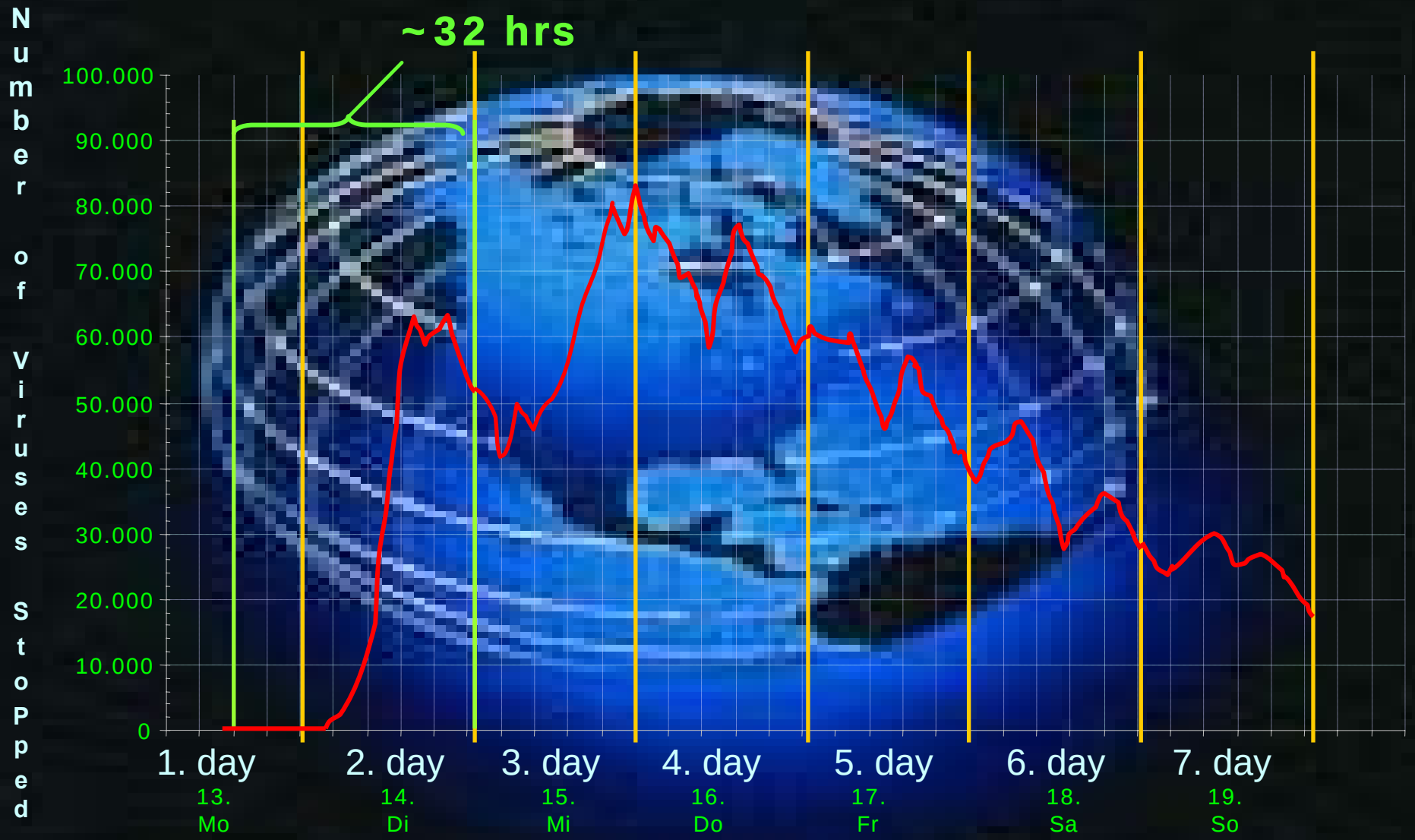
Quelle: www.ikarus.at

Consequences of the preventive measures?



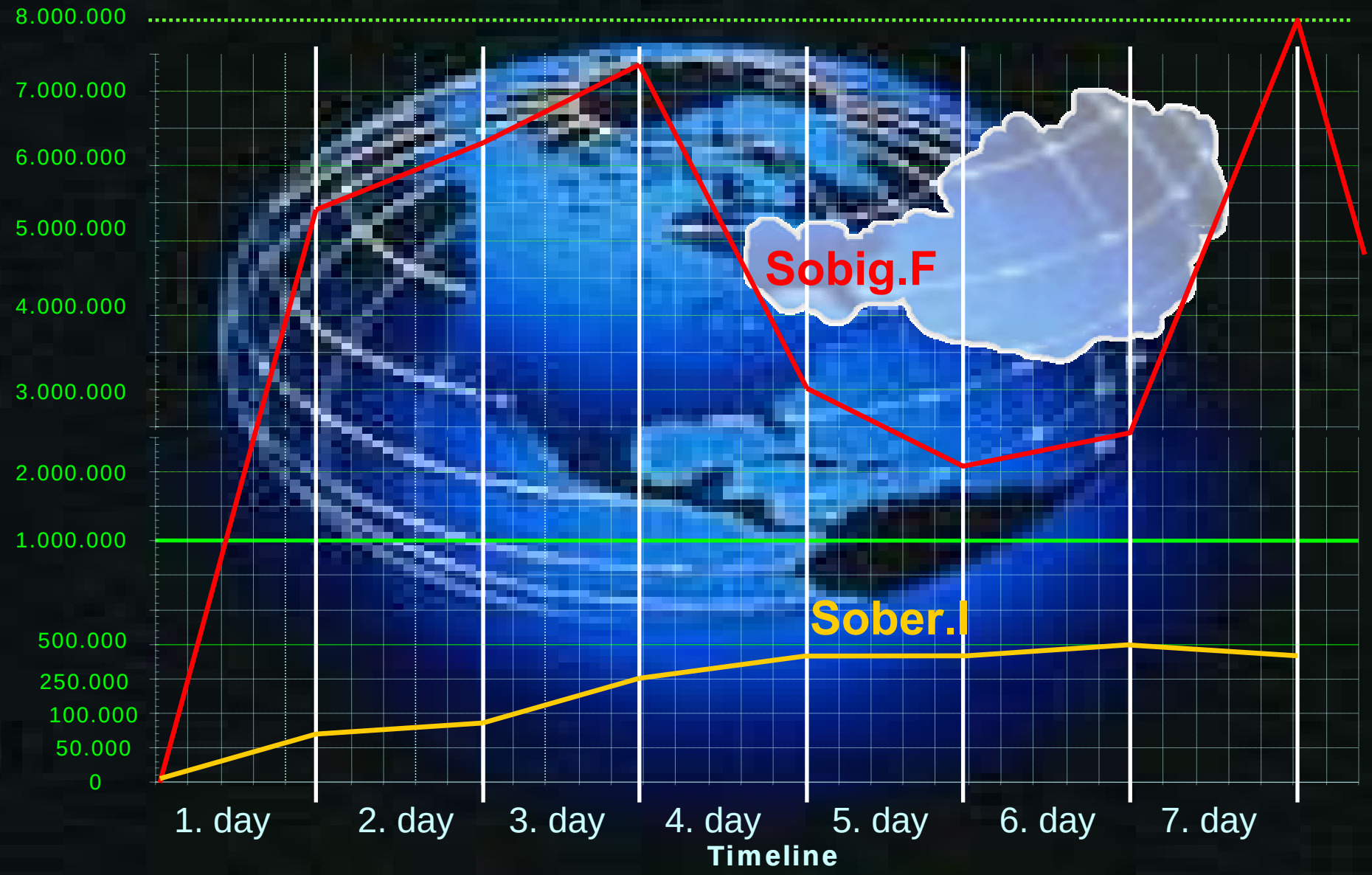
Data courtesy of AV-Test /MessageLabs/Ikarus

Influence of the preventive measures ?



Data courtesy of AV-Test /MessageLabs/Ikarus

Influence of the preventive measures



Conclusion



- Factor Time
- Sensors-Diversity
- Sensors-Density
- Communicationstructures
- Responsemanner

Gründe für die Misere



2004 – Security Anforderungen



45 Patches von Microsoft	3 / Monat
102 dringliche CERT Advisories	8 / Monat
374Updates von AV-Software	31 / Monat
222 Updates von AV-Software 1Q 2005	**74 / Monat**
2580 verschiedene Security-Notes publiziert	215 / Monat
3780 Vulnerabilities von CERT registriert	315 / Monat

Ergibt: 20 erforderliche Reaktionen pro TAG

---

20 erforderliche Reaktionen pro TAG

KARUS SOFTWARE

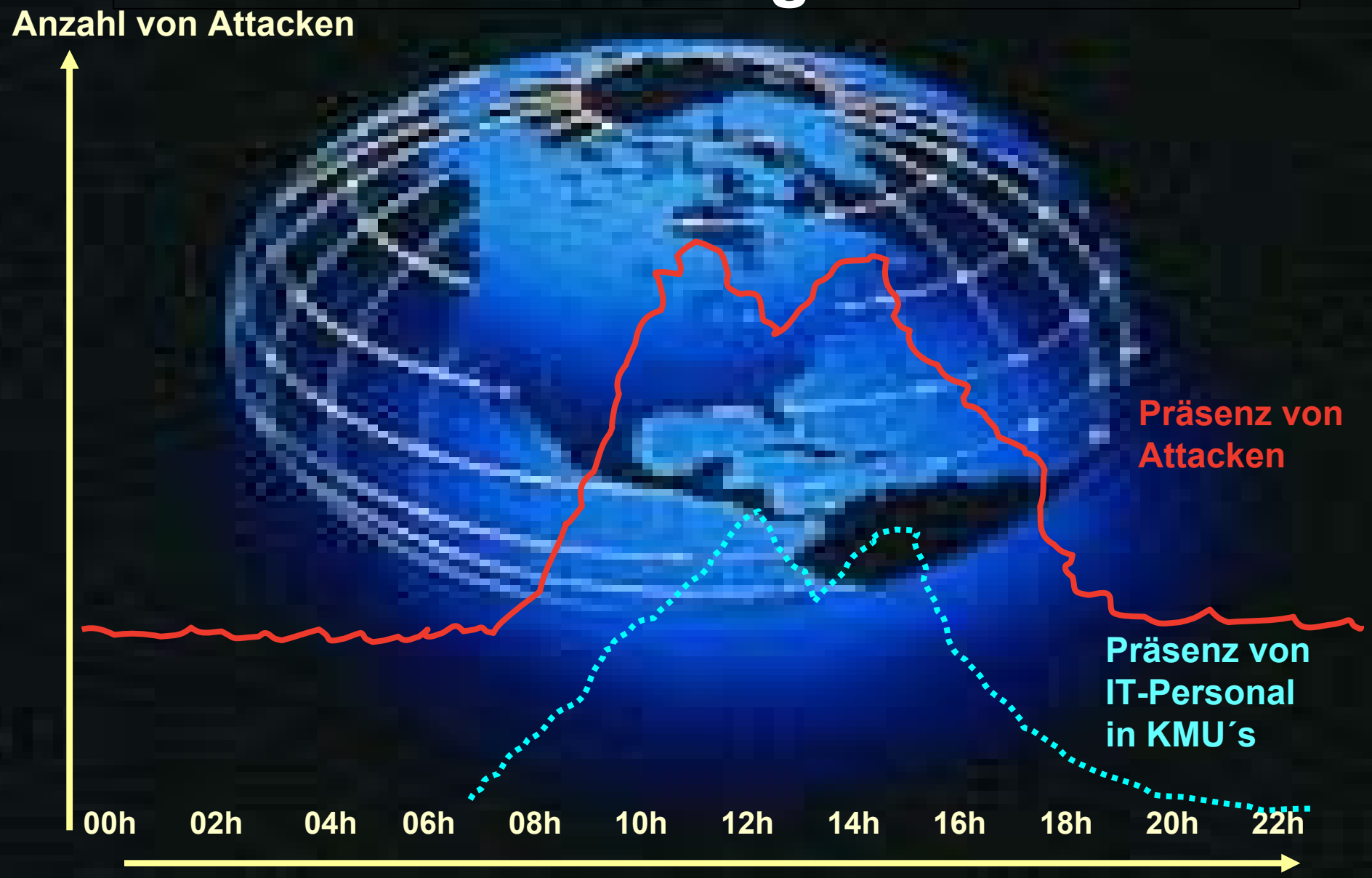
vorausgesetzt:

- Sie verfügen über entsprechendes Know-how in allen betroffenen Bereichen
- Sie verfügen über die erforderliche Infra-strukturen
- Sie verfügen über die erforderlichen Mitarbeiter

Denken Sie nach:

Wieviele Aufgaben hat ein Administrator neben Security pro Tag ?

Ressourcen versus Bedrohungsbild



Bearbeiten Ansicht Favoriten Extras ?
Vorwärts Abbrechen Aktualisieren Startseite Suchen Favoriten Verlauf E-Mail Drucken Bearbeiten Diskussion
http://www.google.com/press/zeitgeist.html Wechseln zu
Search PopSwatter Smiley Central Cursor Mania My Info Games Customize My Button Highlight

Google Zeitgeist - Suchmuster, Suchtrends und Überraschungen bei Google

Werfen Sie unten einen Blick auf die Hitliste der meistgefragten Suchen unserer deutschsprachigen Benutzer. Weitere Informationen über beliebte Google-Suchen in aller Welt erhalten Sie im Google Zeitgeist. (Zeitgeist Archiv hier.)

Februar 2004

Meistgesuchte Sangerinnen
Februar 2004

1. christina aguilera
2. paris hilton
3. britney spears
4. janet jackson
5. jennifer lopez

Haufige Suchbegriffe
Februar 2004

1. routenplaner
2. telefonbuch
3. wetter
4. songtexte
5. arbeitsamt
6. witze
7. karneval
8. frisuren
9. billigflüge
10. das örtliche

Suchbegriffe zum Valentinstag - Februar 2004

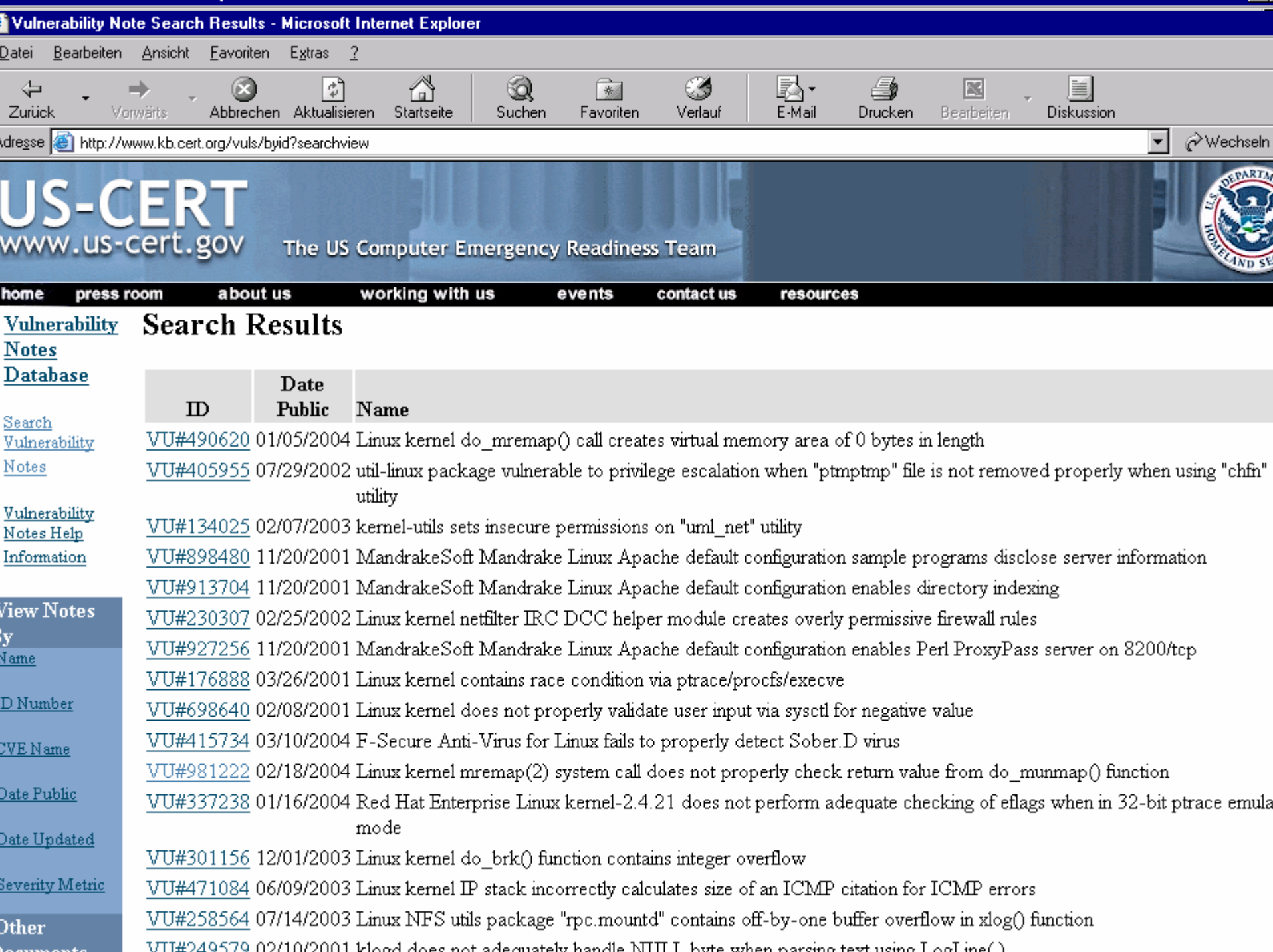
1. valentinstag
2. herz
3. liebe
4. rose
5. valentine's day

Januar 2004

Meistgesuchte Sangerinnen
Januar 2004

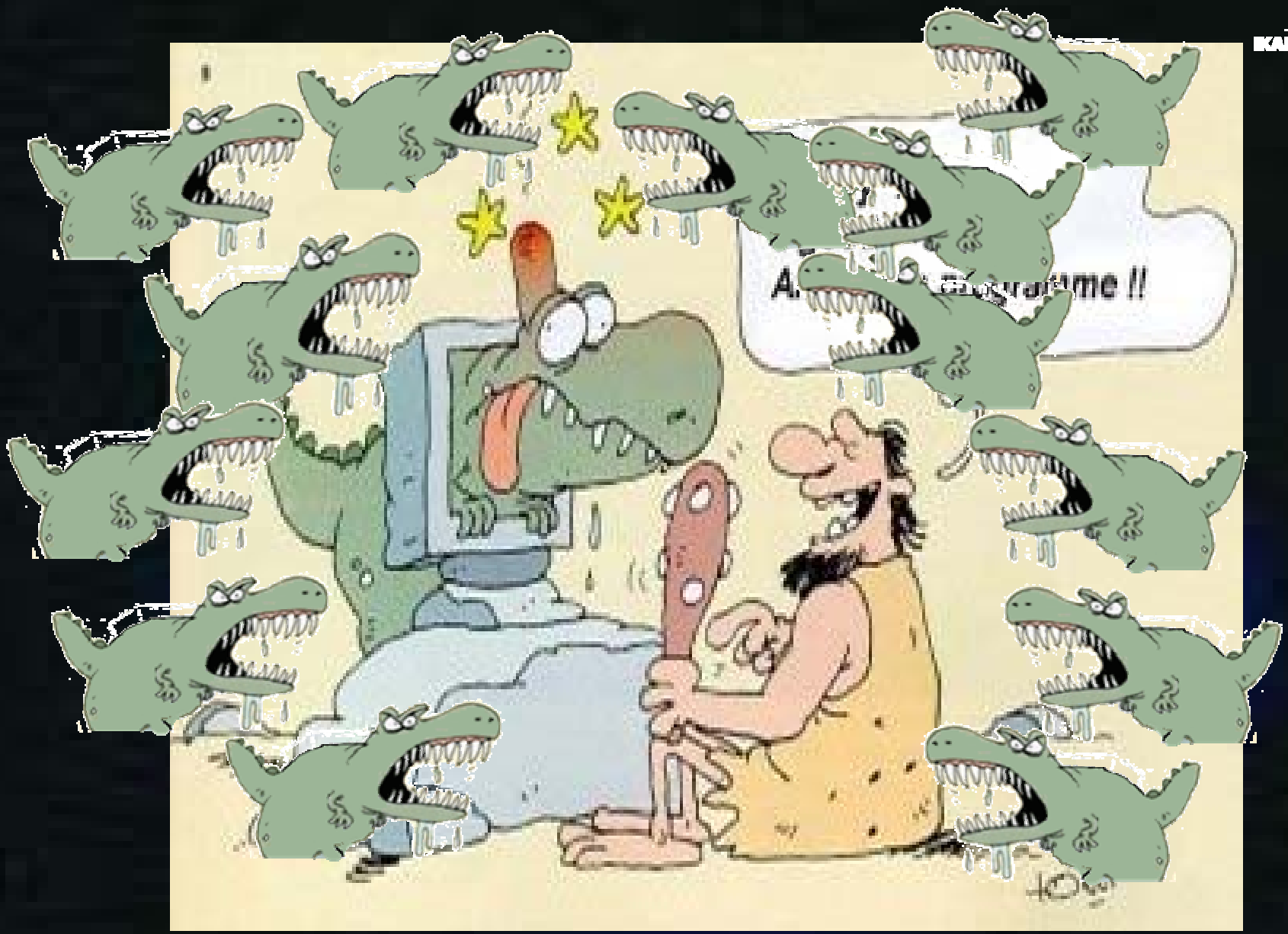
Haufige Suchbegriffe
Januar 2004

Meistgesuchte Marken
Januar 2004

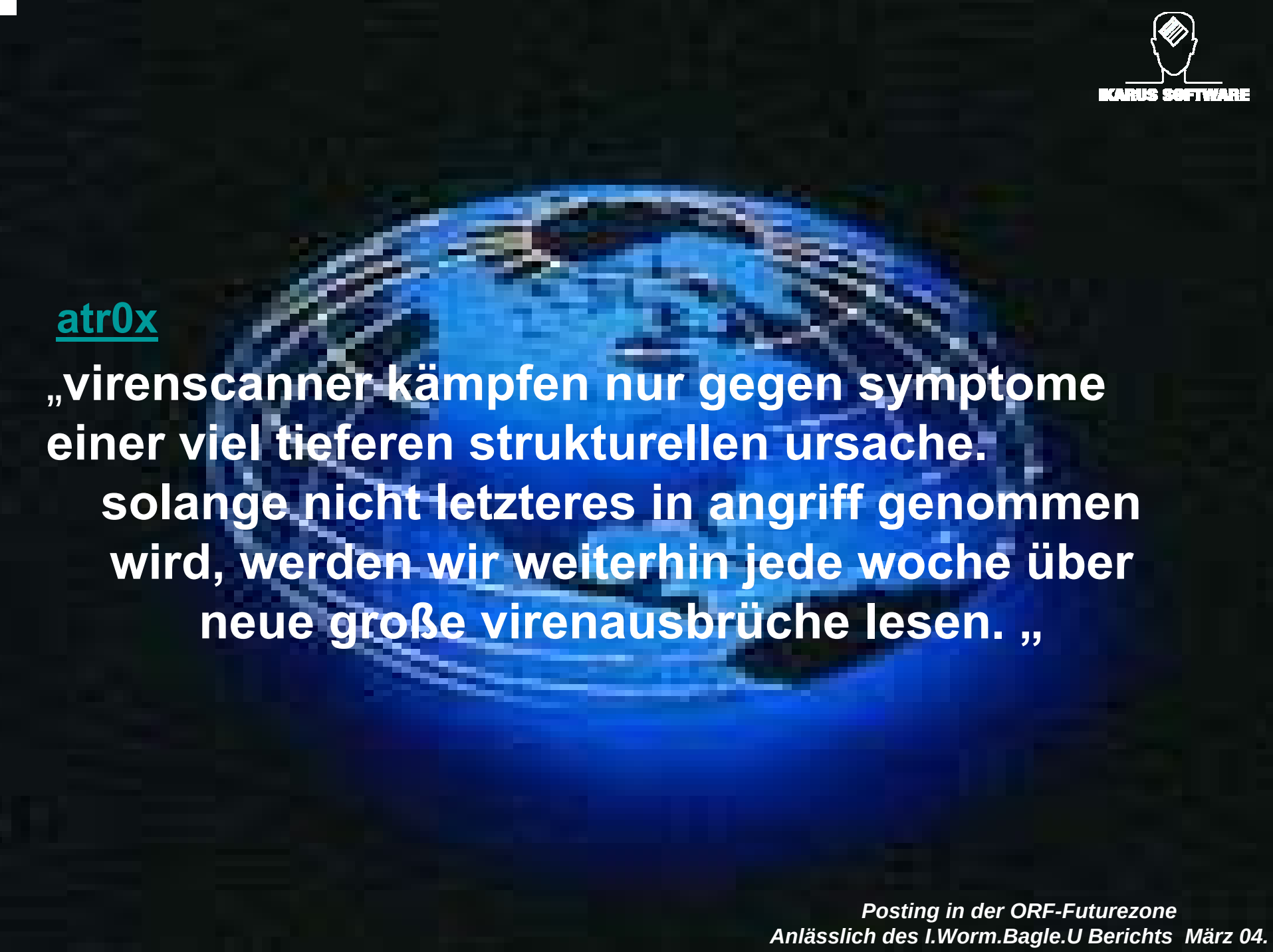


Search Results

ID	Date Public	Name
VU#490620	01/05/2004	Linux kernel do_mremap() call creates virtual memory area of 0 bytes in length
VU#405955	07/29/2002	util-linux package vulnerable to privilege escalation when "ptmptmp" file is not removed properly when using "chfn" utility
VU#134025	02/07/2003	kernel-utils sets insecure permissions on "uml_net" utility
VU#898480	11/20/2001	MandrakeSoft Mandrake Linux Apache default configuration sample programs disclose server information
VU#913704	11/20/2001	MandrakeSoft Mandrake Linux Apache default configuration enables directory indexing
VU#230307	02/25/2002	Linux kernel netfilter IRC DCC helper module creates overly permissive firewall rules
VU#927256	11/20/2001	MandrakeSoft Mandrake Linux Apache default configuration enables Perl ProxyPass server on 8200/tcp
VU#176888	03/26/2001	Linux kernel contains race condition via ptrace/procfs/execve
VU#698640	02/08/2001	Linux kernel does not properly validate user input via sysctl for negative value
VU#415734	03/10/2004	F-Secure Anti-Virus for Linux fails to properly detect Sober.D virus
VU#981222	02/18/2004	Linux kernel mremap(2) system call does not properly check return value from do_munmap() function
VU#337238	01/16/2004	Red Hat Enterprise Linux kernel-2.4.21 does not perform adequate checking of eflags when in 32-bit ptrace emula mode
VU#301156	12/01/2003	Linux kernel do_brk() function contains integer overflow
VU#471084	06/09/2003	Linux kernel IP stack incorrectly calculates size of an ICMP citation for ICMP errors
VU#258564	07/14/2003	Linux NFS utils package "rpc.mountd" contains off-by-one buffer overflow in xlog() function
VU#249579	02/10/2001	klogd does not adequately handle NULL byte when parsing text using LogLine()



IKARUS SOFTWARE



atr0x

„virenscanner kämpfen nur gegen symptome einer viel tieferen strukturellen ursache.
solange nicht letzteres in angriff genommen wird, werden wir weiterhin jede woche über neue große virenausbrüche lesen. „

Posting in der ORF-Futurezone
Anlässlich des I.Worm.Bagle.U Berichts März 04.

Inter/Nationale Virenabwehrnetze

IKARUS SOFTWARE

ISC-SANS, CIRCA

Konzentration der Abwehrmaßnahmen

Providerbasierende Virenfilter

www.uta.at/virenschutz

http://securemail.telekom.at

Hosted Security Services

http://business.telekom.at/produkte/itsolutions/security_service

„Sicherere“ Betriebssysteme

OS-Hardening

Paladium

Awareness

Sicherheitsdenken muss Bestand der Ausbildung werden

Klare Kommunikationsschnittstellen


IKARUS SOFTWARE
DANKE