**Zeitschrift:** Comtec : Informations- und Telekommunikationstechnologie = information and telecommunication technology

**Herausgeber:** Swisscom

**Band:** 81 (2003)

**Heft:** 1

**Artikel:** Klez : der Wurm des Jahres

**Autor:** [s. n.]

**DOI:** https://doi.org/10.5169/seals-876605

# Klez – der Wurm des Jahres

**Klez führte die Viren-Topten von Sophos im letzten Jahr sieben Monate in Folge an und ist damit offiziell der am meisten verbreitete Wurm des Jahres. Laut Sophos, einem führenden Virenschutz-Unternehmen, gingen im Jahr 2002 fast 25% aller Virenvorfälle auf den Klez-Wurm zurück.**

Auf Platz zwei folgte der Bugbear-Wurm, obwohl er erst im Oktober 2002 entdeckt wurde. Badtrans «eroberte» sich den dritten Platz. Dabei handelt es sich um einen Wurm, der Passwörter stiehlt und erstmals im November 2001 auftrat. Trotz des grossen Aufruhrs, auch unter Herstellern von Anti-Viren-Software, sind 2002 keine Viren entdeckt worden, die PDAs oder Mobiltelefone attackieren.

Viren-Autoren wenden häufig psychologische Tricks an: Sie versprechen beispielsweise einen Blick auf Britney Spears, Shakira und Bill Clinton, um Anwender dazu zu bringen, den schädlichen Code zu aktivieren. Jedoch zeigt sich, dass sich Anwender dieser psychologischen Tricks langsam bewusst werden, denn keiner dieser Würmer richtete grossen Schaden an.

### Virenschutz allzeit aktuell

Vireninformationen, die sich selbst automatisch aktualisieren, können auf die eigene Website gestellt werden.
Info: Sophos GmbH,
Tel. +49 (0) 6136 9119-3, Homepage:
www.sophos.de/virusinfo/infofeed/

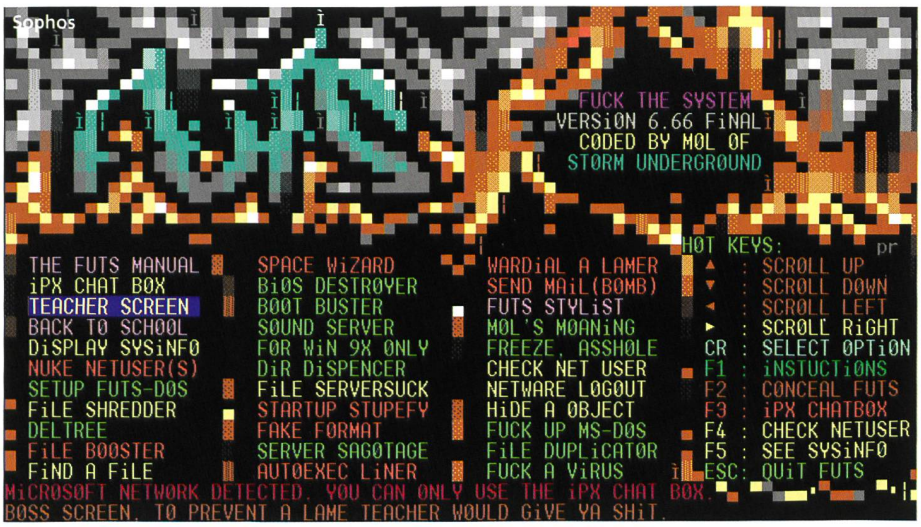
### Virencharts 2002

Neun Viren der Viren-Topten 2002 waren Mass-Mailing-Windows-32-Viren. Die einzige Ausnahme bildete Elkern, der vom Klez-Virus eingeschleust wurde. 87% der Virenmeldungen gingen im letzten Jahr auf Windows-32-Viren zurück. Bis heute erkannte «Sophos Anti-Virus» im Jahr 2002 7189 neue Viren, Würmer und Trojaner. Die Gesamtzahl der Viren, die Sophos bis jetzt aufgespürt und gegen die das Unternehmen Schutzmechanismen zur Verfügung gestellt hat, beträgt damit mehr als 78 000. Im Durchschnitt entwickelt das Virenlabor von Sophos täglich Schutzmechanismen gegen mehr als 25 neue Viren.

Für das Jahr 2002 ergibt sich folgende Rangliste der am häufigsten aufgetretenen Viren:

| | | |
|---|---|---|
| 1. W32/Klez | (Klez-Wurm) | 24,1% |
| 2. W32/Bugbear | (Bugbear-Wurm) | 17,5% |
| 3. W32/Badtrans | (Badtrans-Wurm) | 14,6% |
| 4. W32/Elkern | (Elkern-Virus) | 4,6% |
| 5. W32/Magistr | (Magistr-Wurm) | 4,2% |
| 6. W32/MyParty | (MyParty-Wurm) | 2,2% |
| 7. W32/Sircam | (Sircam-Wurm) | 2,0% |
| 8. W32/Yaha | (Yaha-Wurm) | 1,9% |
| 9. W32/Frethem-Fam | (Frethem-Fam-Wurm) | 1,4% |
| 10. W32/Nimda | (Nimda-Wurm) | 1,2% |
| Andere | | 26,3% |

Im Gegensatz zu früheren Spitzenreitern, wie beispielsweise LoveBug, die meist fast so schnell von der Bildfläche verschwanden wie sie auftauchten, ist Klez einer der Würmer, der sich extrem langsam, aber sicher an die Spitze vorarbeitet. «Er hat es geschafft, Anwender das ganze Jahr hindurch immer wieder zu befallen», erklärt Gernot Hacker, Senior Technical Consultant bei Sophos. «Einen Schutz gegen Klez gibt es bereits seit dem ersten Tag seiner Entdeckung. Die einzige Erklärung für seinen andauernden Erfolg ist, dass manche Anwender ständig versäumen, ihre Anti-Viren-Software zu aktualisieren».



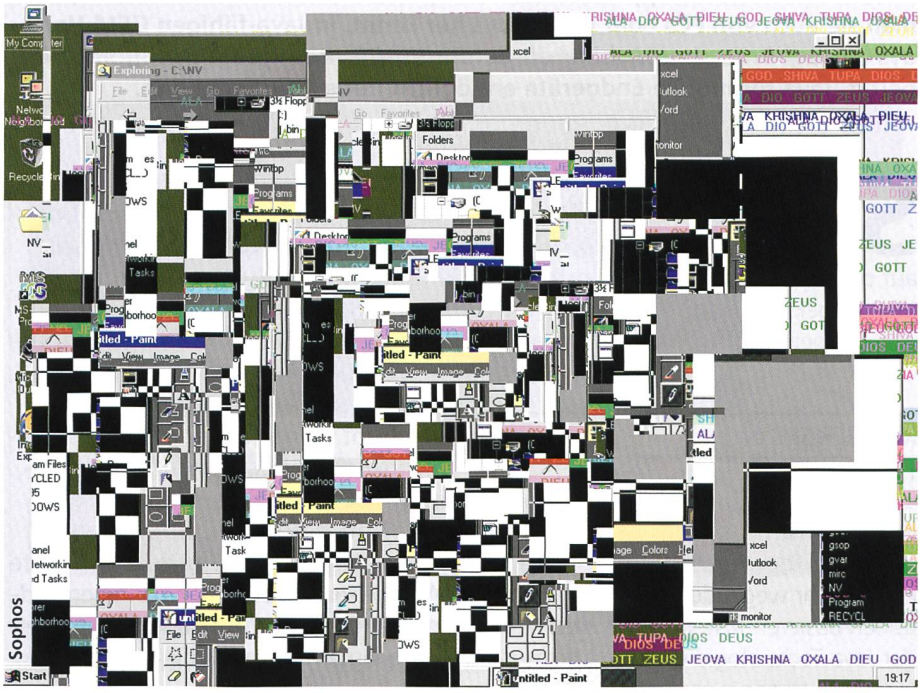
**Weitere Entwicklungen im Jahr 2002**
Würmer machen sich «falsche Adressen» zu Nutze. Bekannte Windows-32-Viren, wie Klez und Yaha, ersetzten die E-Mail-Adresse des Wurmsenders mit einer anderen legitimen E-Mail-Adresse. Dies führte zu einer Flut von Beschwerden darüber, dass unschuldige Anwender Würmer an Kunden, Lieferanten oder Kollegen verschickt haben sollen. Auch Mac-Anwender wurden beschuldigt, den Klez-Wurm verschickt zu haben, obwohl es unmöglich ist, dass ein Mac infiziert ist. Dadurch wurden einige Sicherheits-Unternehmen in ärgste Verlegenheit gebracht, da sie fälschlicherweise Anwender beschuldigten, Viren weiterverbreitet zu haben.
Die folgenden Spezialwürmer haben ebenfalls für einige Unruhe gesorgt:

***Hoaxes***
Der JDBGMGR-Hoax – eine E-Mail, die Anwender dazu bringt, legitime Dateien von ihrem PC zu löschen – wurde erstmals im April 2002 entdeckt und führt die Hoaxes-Rangliste von Sophos seit Mai 2002 stetig an. Die Buchstabenreihe «JDBGMGR» war 2002 der zweitmeist gesuchte Begriff der Sophos-Website. Dieser Suchbegriff wurde nur noch von Klez übertroffen. Obwohl Hoaxes keine schädlichen Codes enthalten, warnt Sophos, dass sie meist genauso wie ein Virus Bandbreiten vergeuden, Mail-Server verstopfen und Anwender verwirren. Richtlinien für einen sicheren Umgang mit Hoaxes sind unter der Homepage: www.sophos.de/safecomputing/ zu finden.

***Der Slapper-Wurm***
Der Linux-Wurm beweist, dass Schwachstellen nicht nur ein Problem von Microsoft sind. Der Slapper-Wurm, der erstmals im September auftrat, machte sich eine bekannte Schwachstelle des Linux-Betriebssystems zu Nutze. Der Virus konnte sich aber letztlich nur so erfolgreich über lokale Netzwerke verbreiten, weil einige Linux-Anwender keine Patches gegen die bekannten Schwachstellen heruntergeladen hatten.

***C#, «Proof of Concept»-Wurm***
Im März ist der Sharp-A-Wurm, der erste Wurm, der in der neusten Programmiersprache von Microsoft, C#, geschrieben wurde, aufgetaucht. Er wurde direkt an Anti-Viren-Hersteller geschickt, um zu beweisen, dass es möglich ist, einen Virus in dieser Programmiersprache zu schreiben. Der Virus wird dem Autor «Gigabyte» zugeschrieben, hinter dem wahrscheinlich eine weibliche Virenautorin steckt.

***Neuer Instant-Messaging-Wurm***
Auch wenn Windows-32-Viren in der Rangliste 2002 klar dominieren, scheint der CoolNow-Wurm, der sich über die Instant-Messaging-Plattform verbreitet, ein Denkzettel dafür zu sein, dass nicht alle Viren via E-Mail kommen. Anwender, die sich nur auf Anti-Viren-Lösungen für E-Mails verlassen, sind folglich nicht vor allen schädlichen Codes geschützt.




**Cyberkriminelle vor Gericht**
Im Mai wurde David L. Smith, der Autor des Melissa-Wurms, der für viele als Vorlage für weitere E-Mail-fähige Würmer diente, in den USA zu einer zwanzigmonatigen Haftstrafe und einer Geldstrafe von insgesamt 7500 US-$ verurteilt.
In Grossbritannien wurde der «Surbiton Hacker» (dessen Name noch nicht bekannt ist) wegen der Entwicklung eines Hacker-Tools für Linux verurteilt. Eine gemeinsame Ermittlung von Scotland Yard und dem FBI hatte den Hacker aufgespürt. Der in Llandudno ansässige Simon Vallor wurde ebenfalls verhaftet und angeklagt, drei Mass-Mailing-Würmer, einschliesslich des Gokar-Wurms, entwickelt und verbreitet zu haben. Im Dezember 2002 musste er sich vor Gericht verantworten. Zudem drängt die US-Regierung derzeit auf die Auslieferung von Gary McKinnon aus London, der vertrauliche Netzwerke der Regierung und des Militärs angegriffen haben soll.

**Prognose für 2003**
Laut Sophos wird sich der Siegeszug der Windows-32-Viren weiter fortsetzen, da diese Mass-Mailing-Viren die meisten Auswirkungen haben. Wahrscheinlich werden diese Viren falsche Sender-Adressen verwenden, um die Verwirrung der Anwender zu verstärken.
Für gezieltere Attacken erwartet Sophos einen Anstieg der Backdoor-Trojaner. Sie nutzen Schwachstellen in Betriebssystemen aus, um Remote Access Tools (RAT) zu implementieren. Durch RATs können Hackers den Fernzugriff auf infizierte PCs erlangen. Gary McKinnon – angeklagt, sich in das Netzwerk der US-Regierung gehackt zu haben – wird unterstellt, einen RAT implementiert zu haben, um an Passwörter und vertrauliche Informationen zu gelangen.
In Bezug auf Anti-Viren-Lösungen in Unternehmen, erwartet Sophos einen Anstieg an umfassenden Sicherheitstechnologien, um bestimmte gefährliche Dateitypen, die schädliche Codes enthalten können (wie z. B. .exe), gleich am E-Mail-Gateway zu blockieren. 4