

sind in aller Munde – doch auf dem Mac haben nur die wenigsten schon einen **Befall**

erlebt. Kein Grund, sorglos zu sein: Wir zeigen Ihnen, wo die **Ansteckungsgefahr** lauert und wie Sie Ihren Rechner schützen.



Rechner- wahnsinn

Über Computerviren wird häufig berichtet, aber die wenigsten Macianer haben selbst schon mal einen Befall erlebt. Das liegt daran, daß die Großzahl der Viren auf die DOSen-Welt beschränkt ist. Es gibt jedoch auch Ungeziefer, das nur Macs befällt.

BeisoldhenVirenhandeltessichum kleine Programme, die mehr oder weniger raffinierte Hacker entwickelt haben, um andere Programme oder Dateien zu manipulieren und sich dabei ungehemmt fortzupflanzen, sprich: zu kopieren. Die Motive dieser Hacker liegen irgendwo zwischen aufschneiderischer Programmierkunst und boshafter Zerstörungswut; dementspre-





chend reicht das Spektrum dessen, was Viren anrichten können, von harmlosen Gags über das bloße Vergrößern einer Datei bis zum kompletten Datenverlust durch das Löschen der Festplatte. Einen Virenbefall sollten Sie jedoch in gar keinem Fall unterschätzen.

Höchst ansteckend! Wie kommt es überhaupt zu einem solchen Befall? Die Antwort lautet leider: Sehr leicht! Grundsätzlich gilt für Computerviren nämlich dasselbe wie für ihre biologischen Artgenossen: Man sieht sie nicht, und sie vermehren sich bei jeder Gelegenheit. Sie brauchen bloß einmal eine infizierte Diskette von einem Bekannten einzulegen, und schon nistet sich ein Abkömmling auf Ihrer Festplatte ein! Wenn Sie den Mac dann nicht sofort desinfizieren, steht ein ungebremster Befall direkt bevor. Auch über Online-Dienste kann sich Ihr Rechner ein Virus einfangen: Wenn sie eine virale Datei auf die Festplatte laden, ist es schon passiert, Sie haben ebenso unbemerkten wie ungebetenen Besuch.

Gegenmaßnahmen. Genau wie Sie sich im richtigen Leben bei einer durch Viren hervorgerufenen Erkrankung ein

Gegenmittel verschreiben ließen, müssen Sie sich nun für Ihren Mac eine spezielle Anti-Virus-Software besorgen, die ihn von jeglichem digitalen Ungeziefer befreit.

Um ein Virus beseitigen zu können, muß die Software es zunächst erkennen, also bereits für dieses spezielle Virus programmiert sein. Hat der Eindringling aber später das Licht der Welt erblickt als der digitale Virenkiller, wird er nicht erkannt und bleibt unbehelligt. Deshalb werden derartige Programme regelmäßig per Update auf den neuesten Stand an der Virenfront gebracht.

Auch bei Computerviren ist es natürlich besser vorzubeugen als zu heilen. Damit Sie keine virenbefallenen Daten von Online-Diensten, infizierten Disketten oder anderen Speichermedien unbemerkt auf Ihre Festplatte laden, überprüfen Virenschutzprogramme beim Ladevorgang sowohl die einzelnen kopierten Dateien als auch – im Falle von Disketten oder Wechselplatten – die jeweiligen Schreibtischdateien auf eventuellen Befall.

Bestimmte Virenkiller können sogar in komprimierten Datenarchiven nach den Übeltätern suchen, und sie bereits beim Dekomprimieren un-

schädlich machen. Weiterhin überwacht Anti-Virus-Software den Computer in Hinsicht auf verdächtige Vorkommnisse: Wird beispielsweise ein Programm manipuliert, so ändert sich auch die Prüfsumme des *Programmcodes* – verdächtig ist das allemal, denn warum sollte im Programmcode etwas geändert werden? Außerdem erkennen diese Programme gleichartige Veränderungen in verschiedenen Dateien, ein sicherer Hinweis auf ein sich ausbreitendes Virus.

Bloß keine Panik! Nach all diesen Hinweisen sollen Sie jedoch auf keinen Fall in Panik geraten: Macianer scheinen glücklicherweise eine sehr kollegiale Zunft zu sein, denn Viren treten nur sehr selten auf – boshafte Programmierer sind offensichtlich deutlich in der Minderheit. Dennoch empfiehlt es sich immer, einen wirksamen Virenschutz auf Ihrem Rechner zu installieren, damit Sie im Fall der Fälle gewappnet sind. Einen solchen Schutz enthalten beispielsweise auch einige Hilfsprogrammpakete wie MacTools von Central Point – wir stellen Ihnen aber hier die beiden verbreitetsten Virenkiller vor: Die Freeware Disinfectant und den Profikiller SAM. ♦ AM

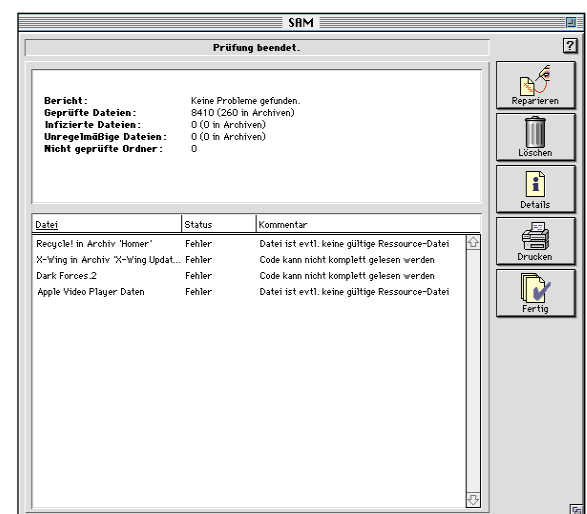
Selbst das umfangreichste Programm besteht im Prinzip nur aus Nullen und Einsen; zählt man diese Zahlen zusammen, so erhält man die sogenannte Prüfsumme, die von den Virencheckern gespeichert werden kann. Wird nun aber der Programmcode geändert, so verändert sich auch die Prüfsumme, da mit an Sicherheit grenzender Wahrscheinlichkeit die Summe der neuen Zahlen nicht mit der alten übereinstimmt.

easyfacts

Der Fall von Troja

■ Exklusiv auf der MACeasy-CD finden Sie die Systemerweiterung **VisibleWasteland**, die das unlängst aufgetretene trojanische Pferd Invisible Oasis erkennt und unschädlich macht. Ein „trojanisches Pferd“ ist ein naher Verwandter von Viren – ein Programm oder eine Systemerweiterung, die sich heimlich ins System schleicht, um von dort aus Informationen auszuspionieren. Derjenige, der das trojanische Pferd platziert hat, kann diese Informationen später abrufen, um so etwa Paßworte herauszufinden. Bei Invisible Oasis handelt es sich um eine unsichtbare Systemerweiterung, die die gesammelten Infos unbemerkt über ein Netzwerk weitergeben kann. Um sie aufzuspüren und zu vernichten, müssen Sie nur VisibleWasteland installieren – eine Systemerweiterung, die im MACup Verlag geschrieben wurde.

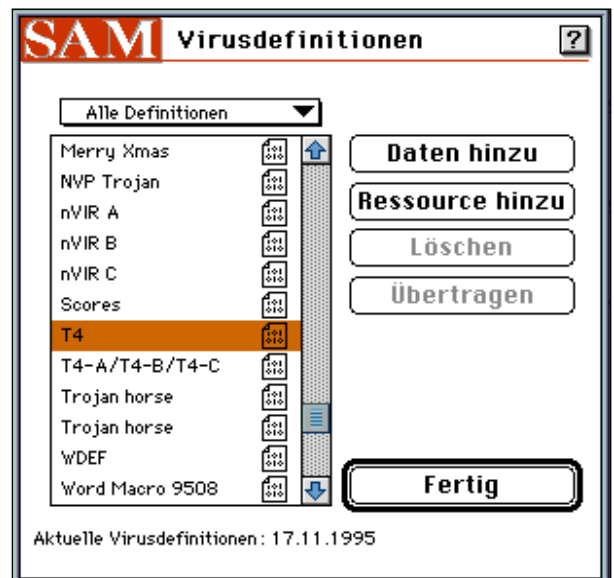
Die Benutzeroberfläche von SAM wirkt professionell. Neben Virenbefall erkennt das Programm fehlerhafte Dateien, ...



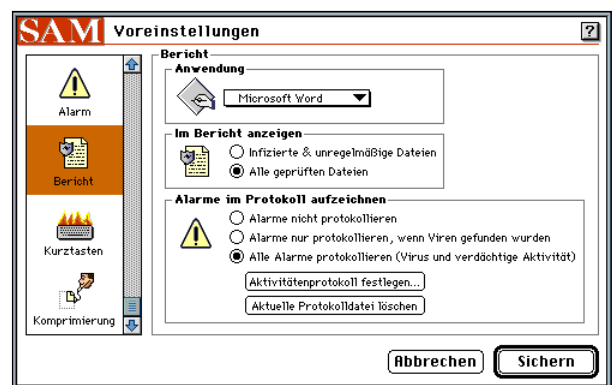
Anti - Virus-Software 1

■ Das kommerzielle Anti-Virus-Programm SAM (Symantec Antivirus for the Macintosh) besitzt eine komfortable Benutzeroberfläche und einen enormen Funktionsumfang. Es erkennt nicht nur Virenbefall, sondern überwacht im Hintergrund auch sämtliche Festplattenzugriffe. Verdächtige Vorkommnisse meldet SAM dann sofort. Die Empfindlichkeit dieser Hintergrundüberwachung läßt sich individuell regulieren, eine hohe Empfindlichkeit erhöht allerdings die Anzahl der Fehlalarme.

Das Softwarepaket besteht aus dem eigentlichen Prüfprogramm, das sogar in komprimierten Archiven nach Viren suchen kann, einer Systemerweiterung zum Überwachen der Hintergrundaktivitäten und dem Programm „Startup Disk Builder“, mit dem sich eine Startdiskette erstellen läßt, um auch die Systemsoftware auf der Festplatte untersuchen und desinfizieren zu können. SAM erkennt neben herkömmlichen und HyperCard-Viren auch trojanische Pferde und merzt diese aus. Damit SAM immer auf dem laufenden bleibt, können Sie entweder eigene Virusdefinitionen manuell eintragen, oder aus dem Internet regelmäßig die neuesten Virendefinitionen unter der Adresse <ftp://ftp.symantec.com> abrufen. Hersteller: Symantec, Preis: zirka 200 Mark im Fachhandel

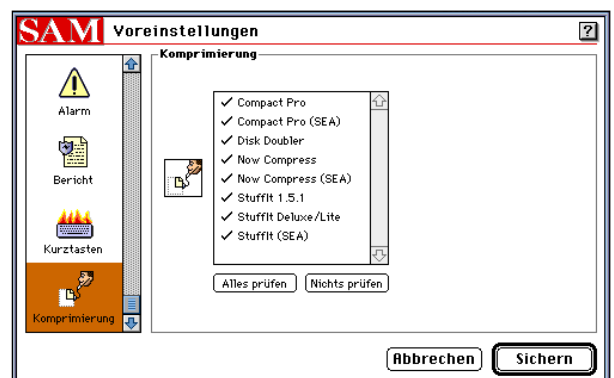
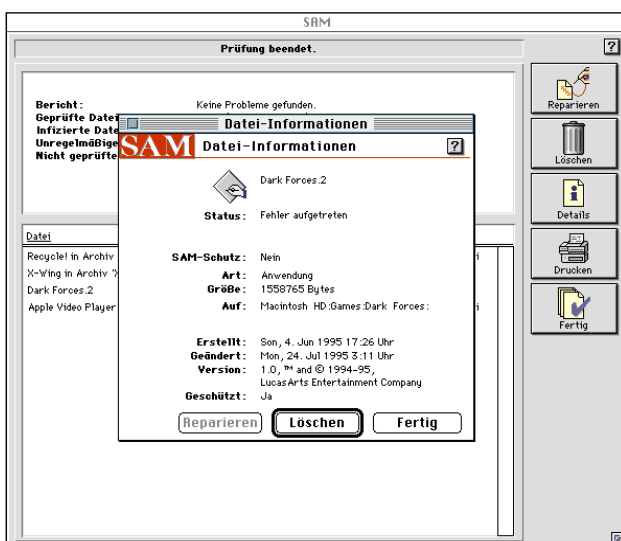


In SAM lassen sich entweder eigene oder aus dem Internet abgerufene Definitionen neuer Viren eintragen (Adresse siehe links).



Über zahlreiche Menüs können Sie SAM genau auf Ihre Bedürfnisse abstimmen, ...

... die man bei Bedarf näher untersuchen kann.



... um beispielsweise selbst komprimierte Daten auf Viren zu durchforsten.

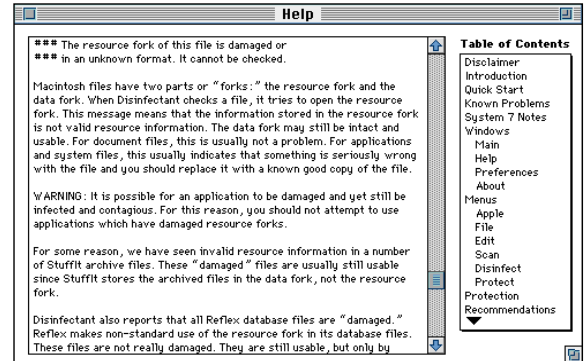
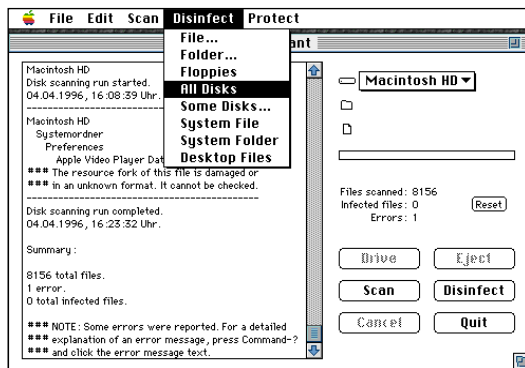
Disinfectant 3.6

Anti-Virus-Software 2

■ Obwohl Disinfectant ein Freeware-Programm ist – der Autor also kein Geld dafür verlangt –, ist es ein effektiver und zuverlässiger Virenkiller mit einer etwas holprigen, aber funktionellen Benutzeroberfläche. An einer amerikanischen Universität geschrieben, wird es durch regelmäßige Updates über das Internet ständig auf dem aktuellen Stand gehalten. Es erkennt keine HyperCard-Viren, bietet aber neben der kompletten Festplattenuntersuchung und -reinigung auch eine Systemerweiterung, die sowohl Disketten und Wechselplatten als auch Online-Daten beim Laden überprüfen kann.

Bezug über <http://ciac.llnl.gov/ciac/ToolsMacVirus.html>

Autor: John Norstadt, Preis: kostenlos



Auf Nachfrage erfahren Sie von Disinfectant 3.6 alles Wissenswerte über Viren, Macs und wie Sie einen Befall verhindern können.

Der Bedienkomfort des Virenkillers Disinfectant 3.6 fällt ziemlich spärlich aus, die gebotenen Kontrollmöglichkeiten sind aber ausreichend.

easyfacts

Mac-Viren: Die sechs miesesten

- 1 **CODE-1:** Wenn Sie Ihren infizierten Rechner an einem 31. Oktober (Halloween) starten, so wird Ihre Festplatte in „Trent Saburo“ umbenannt. Da das Virus aber schlecht programmiert ist, kommt es in vielen Fällen auch zu fatalen Systemabstürzen.
- 2 **CODE 252:** Zwischen dem 6. Juni und dem 31. Dezember zündet dieses Virus: Auf dem Bildschirm erscheint die Meldung „Sie haben ein Virus! Hahahahahaha! Alle Daten werden jetzt gelöscht! Hahahahaha! P.S.: Einen schönen Tag noch! Hahahaha! (zum Fortfahren bitte klicken)“ – danach löscht sich das Virus von der Festplatte. Sie verstehen richtig: Dieses Virus richtet keinerlei Schaden an – sollte Ihr Rechner befallen sein, so bewahren Sie einfach die Ruhe, denn durch hektisches Steckerziehen würden Sie in diesem Moment Ihre Daten wahrscheinlich eher selbst gefährden!
- 3 **INIT-9403:** Dieses Virus, das bis jetzt nur italienische Systeme angefallen hat, beginnt nach einer gewissen Zeit, sämtliche Festplatten und Disketten mit Nullen zu überschreiben und somit alle darauf enthaltenen Daten zu zerstören.
- 4 **INIT M:** An einem Freitag, dem 13. beginnt dieses Virus, alle Dateien auf der Festplatte mit Fantasienamen umzubenennen, und somit für den Benutzer unbrauchbar zu machen: Man kann seine Daten und Programme nicht wiederfinden!
- 5 **nVIR A/nVIR B:** Diese beiden Viren setzen sich im System fest, um nach jedem achten oder sechzehnten Neustart einen Warnton auszusenden. Haben Sie die Sprach-Software MacIntalk installiert, erklingt statt des Warntons der Satz „Don't panic!“. Hinterhältigerweise sind nVIR A und nVIR B auch sexuell aktiv. Wenn sich beide Varianten auf einem Rechner befinden, fangen sie an sich zu „paaren“, das heißt Teile des einen Virus verbinden sich mit Teilen des anderen; auf diese Weise erschweren sie ihre Erkennbarkeit für Anti-Virus-Programme.
- 6 **WM 9509:** Bei diesem im letzten September entdeckten Virus handelt es sich streng genommen ein Word-6-Makro, folglich können nur solche Macs infiziert werden, auf denen dieses Programm installiert ist. Neben destruktiven Aktivitäten hängt es an das Ende eines gedruckten oder gefaxten Dokuments die Sätze „And I finally would like to say: Stop all French nuclear testing in the Pacific!“ Disinfectant 3.6 und SAM 4.0 können die sechs Viren erkennen und beseitigen.