von Janko Röttgers *am 30.08.2001*

Sie lieben uns.txt.vbs

Virenprogrammierer: Ihre Geschichte, ihre Communities, ihr Katz- und Mausspiel mit der Antivirus-Industrie

"Sachen zu sammeln ist etwas, was ich immer gern gemacht habe. Als Kind sammelte ich Briefmarken, jetzt sammle ich Computerviren." Luis ist 27, glücklich verheiratet, arbeitet in einem spanischen IT-Unternehmen und widmet sich in seiner Freizeit mit Vorliebe Programmen, um die andere Computernutzer lieber einen großen Bogen machen.

Virensammler wie Luis gibt es ein paar wahrscheinlich hunderte. Doch nur wenige nehmen dieses Hobby so ernst wie er, und niemand besitzt eine derart große Sammlung. Wie viele elektronische Schädlinge auf seiner Festplatte schlummern, möchte er nicht sagen. Luis ist in solchen Beziehungen sehr genau. Er weiß, dass viel Unsinn über die Zahl der existierenden Viren geschrieben wird. Er weiß, dass die Hersteller von Antivirus-Software sich gegenseitig mit Zahlen zu überbieten versuchen, die jenseits von gut und böse liegen. Luis möchte diese Diskussion nicht noch weiter anstacheln. Er verrät nur so viel: Lediglich drei oder vier der größten Hersteller von Antivirus-Software besäßen eine größere Sammlung als er. Letztlich geht es ihm aber auch gar nicht um die Größe der Sammlung, sondern um jedes einzelne Exemplar. Ein echter Sammler eben.

Seit fast zehn Jahren ist Luis nun schon unter dem Namen Virusbuster Teil einer vitalen Szene des elektronischen Undergrounds, die sich selbst als vXer bezeichnen. Virenprogrammierer, Virensammler und andere Freunde sich selbst vervielfältigender Programme, die sich in kleinen Gruppen zusammenschließen und über ein eng gesponnenes Netzwerk aus Chaträumen, Websites und elektronischen Magazinen austauschen. Luis ist Mitglied der 29a-Gruppe, gegründet 1996 von einem spanischen Programmierer mit dem Pseudonym Mr. Sandman. 29a gilt sowohl unter vXern als auch unter Mitarbeitern von Antivirus-Softwarefirmen - vXer nennen sie gerne AVler - als eine der innovativsten Gruppen der Szene. Der erste Windows-2000-Virus, der erste Gnutella-Wurm, der erste Plattform-übergreifende Virus, der sowohl Windows als auch Linux infiziert - 29a lotet ständig neue Möglichkeiten für elektronische Schädlinge aus. Ständig zwingt sie damit auch die Programmierer von Antivirus-Software, ihre eigenen Programme zu verfeinern und die ihnen zu Grunde liegenden Konzepte zu überdenken. Ein ewiges Katz- und Mausspiel.

Würmer, Kaninchen und geklonte Elche

Es ist ein Spiel mit Tradition, das Luis und seine Freunde da spielen. Die ersten programmierten Schädlinge tauchen bereits in den Sechzigern auf einigen Großrechnern auf. Sie vervielfältigen sich selbst im Hauptspeicher der Maschinen, klauen damit anderen Nutzern die zu dieser Zeit noch so kostbare Rechenzeit und werden wegen ihres Vermehrungsdrangs Kaninchen genannt.

Anfang der Siebziger experimentiert dann ein gewisser Bob Thomas mit einem Programm, das sich innerhalb eines Netzwerks von Rechner zu Rechner fortbewegen kann. Thomas arbeitet beim ARPANET-Entwickler Beranek and Newman und ist dort aktiv an der Entwicklung der technischen Grundlagen des heutigen Internets beteiligt. Im wahrsten Sinne des Wortes ein Job mit Zukunft. Einer, den man gerne behalten will. Dummerweise erweist sich sein kleines Experiment - Thomas hat das Programm Creeper getauft - als äußerst erfolgreich. Es pflanzt sich im Tenex-Netzwerk der Firma unkontrolliert von Rechner zu Rechner fort und scheint nicht mehr zu stoppen. Kurzerhand programmiert Thomas ein zweites Programm namens Reeper,

das dem Schädling nachjagt und ihn erfolgreich ausschaltet.

Reeper ist damit gewissermaßen die erste Antiviren-Software der Welt. Allerdings würden Antivirus-Experten Creeper aus heutiger Sicht nicht Virus nennen, da das Programm keine anderen Dateien infiziert, sondern sich nur selbst autonom im Netzwerk fortpflanzt. Solche Geschöpfe nennt man heute Wurm - ein Begriff, den John Hupp und John Shoch vom Xerox Palo Alto Research Center 1982 einführen. Die beiden Science Fiction-begeisterten Forscher lassen sich dabei von John Brunners Kultbuch "Der Schockwellenreiter" inspirieren. Brunner spricht darin schon Mitte der Siebziger von einem "Tape worm" - einem sich selbst vervielfältigenden Programm, mit dem der Held des Romans das Computersystem einer totalitären Regierung lahm legt.

In den Jahren 1981 und 1982 entwickeln einige Computer-begeisterte Jugendliche dann das, was man als erste Computerviren bezeichnen kann. Der fünfzehnjährige College-Freshman Rich Skrenta schreibt ein Programm für den Apple 2 mit dem schönen Namen Elk Cloner. Der sich selbst vervielfältigende Elch infiziert Disketten mit dem Apple Disk Operating System 3.3, ohne dabei Daten zu löschen. Startet man eine solche infizierte Diskette zum fünfzigsten Mal, erscheint ein kleines Gedicht auf dem Bildschirm:

"It will get on all your disks
It will infiltrate your chips
Yes it's cloner!

It will stick to you like glue
It will modify RAM too
Send in the Cloner!"

Später wird Rich Skrenta Mitgründer des Open Directory Projects. Das er den wohl ersten Virus geschrieben hat, hängt ihm allerdings heute noch nach: "Der dümmste Hack den ich je programmiert habe, aber er erzeugte am meisten Aufmerksamkeit", erklärt er dazu Jahre später.

Joe Dellinger studiert zu dieser Zeit an der Texas A&M University und spielt ebenfalls viel mit dem Apple 2 herum. Er schreibt wie Skrenta einige sich selbst vervielfältigende Programme. Ohne groß darüber nachzudenken, nennt er sie Virus1, Virus2 und Virus3 und besetzt damit einen Begriff, der uns bis heute begleitet.

Fred Cohen: Jedes System ist infizierbar

Durchsetzen sollte sich dieser Begriff aber erst, als Fred Cohen 1984 seine Forschungsergebnisse mit sich selbst vervielfältigenden Programmen unter dem Titel "Computer Viruses - Theory and Experiments" veröffentlicht. Cohen definiert hier erstmals, was genau eigentlich ein Computervirus ist: ein sich selbst vervielfältigendes Programm, das andere infizieren kann, indem es ihnen den eigenen Code einverleibt. Cohen liefert in seiner Abschlussarbeit gleich auch einige geringfügig abstrahierte Beispiele für den Aufbau eines solchen Viruses mit - ein Schritt, der heute wohl manch einen Professor zum Ablehnen der Arbeit bewegen würde.

Doch 1984 gibt es noch keine bösen Viren, keine Underground-Szene der Virenprogrammierer, keine Antivirus-Industrie und keine sensationsheischenden Zeitungsartikel. Wenn ein Virus Schaden anrichtet, dann allenfalls durch Unachtsamkeit und schlechte Programmierung. Wer in diesen Tagen etwas über Viren lehren oder lernen will, muss ganz zwangsläufig auch welche programmieren. Trotzdem ahnt Cohen bereits, dass man eines Tages Schutz vor Viren und Würmern brauchen wird, dass sie zur Bedrohung werden können.

Er überprüft mögliche Sicherheitskonzepte auf ihre Wirksamkeit, stellt aber bald fest: Vollkommene Sicherheit verspricht nur ein komplett abgeschlossenes System. Eines, das ohne Code von außen auskommt, nicht vernetzt ist und möglichst auch gar keine Eingaben zulässt. Sicher nicht das, was man von einem Computer erwartet. Alle anderen Systeme seien für Viren anfällig, so Cohen. Dies gelte auch für noch zu entwickelnde Systeme, denn: "Die vorgestellten Ergebnisse sind nicht Betriebssystems- oder Implemen-

tations-spezifisch, sondern basieren auf den grundlegenden Eigenschaften von Systemen." Mit anderen Worten: Es gibt keinen absoluten Schutz vor Viren. Jeder Rechner, jedes System kann infiziert werden.

Die ersten Viren mit Impressum

Einige Systeme allerdings leichter als andere, wie sich bald zeigen wird. Im März 1982 erscheint die erste Version von Microsofts MS DOS. Dank eines geschickt ausgehandelten Vertrags mit IBM legt Firmengründer Bill Gates den Grundstein dafür, dass dieses System binnen weniger Jahre zum Standard für Desktop-PCs wird. Und dank seiner Architektur, die keinerlei Privilegien und Schutzmechanismen kennt, wird es bald zur wichtigsten Plattform der Virenprogrammierer.

1986 verbreitet sich erstmals ein MS DOS-Virus um den Erdball. Die beiden Brüder Basit und Amjad Farooq Alvi besitzen eine kleine Softwarefirma namens Brain Computer Services in Pakistans Hauptstadt Lahore. Um gegen die immense Raubkopiererei in ihrem Land vorzugehen, programmieren sie den ganz und gar harmlosen Brain-Virus. Überrascht müssen sie allerdings feststellen, dass schon kurze Zeit später auf der ganzen Welt Disketten verbreitet werden, in deren Boot-Sektor sich ihr Virus findet - und mit ihm die gültige Adresse und Telefonnummer der beiden.

Ebenfalls ganz brav mit seinem echten Namen und seiner Telefonnummer kennzeichnet der deutsche Programmierer Ralf Burger seine ersten Viren. Mit seinem Virdem-Virus im Gepäck besucht er 1986 den Chaos Communication Congress, den der Chaos Computer Club jährlich organisiert. Viren bilden in diesem Jahr das Schwerpunktthema der Veranstaltung. Erstmals kann sich eine breitere interessierte Öffentlichkeit über das Phänomen informieren. Angeblich beteiligen sich bis zu 20 aktive Virenprogrammierer an den angebotenen Workshops. Die Szene formiert sich.

Ab etwa 1987 tauchen immer mehr Viren für MS DOS-Rechner auf. Den Programmierern geht es längst nicht mehr nur um das reine Selbst-Vervielfältigen. Ihre Geschöpfe mit Namen wie Cascade-Virus, Vienna-Virus oder Jerusalem-Virus unterscheiden sich auch in dem, was sie mit dem befallenen Rechner anrichten - den so genannten Payloads. Burgers Virdem-Virus fordert den Benutzer irgendwann auf, eine Zahl zu raten. Nur wer richtig liegt, darf weiterarbeiten. Der Stoned-Virus wird dadurch berühmt, dass er verkündet: "Your PC is stoned!" Doch einige Programmierer bedienen sich auch nur der bereits verbreiteten Viren-Quellcodes, um mit gefährlichen Payloads ihrer destruktiven Energie freien Lauf zu lassen. Eine Variante von Burgers Virdem-Virus etwa formatiert am Freitag dem dreizehnten die befallene Festplatte. Neben solch bösen Überraschungen entwickeln die Virenprogrammierer auch erste Techniken zur Verschleierung ihrer Aktivitäten. Der Cascade-Virus beispielsweise setzt auf Verschlüsselung - ein klares Tribut an die noch junge Antivirus-Industrie.

Mit Ghostbuster-Attitüde gegen elektronische Schädlinge

Eine der schillerndsten Gestalten dieser Branche ist zu dieser Zeit John McAfee, Chef der Firma Interpath und später Gründer von McAfee Associates. 1988 gründet er den Branchenverband "Computer Virus Industry Association". Zahlreiche Antivirus-Firmen wollen jedoch nicht beitreten, weil sie McAfee bezichtigen, als Gründer des National Bulletin Board Society-Netzwerks selbst Viren zu verbreiten. Auch wenn ihm dieser Vorwurf unter Experten noch über Jahre nachhängt, schafft Mcafee es, in den Augen der Öffentlichkeit zum prominentesten aller Virenjäger zu werden.

Der für seine Utility-Sammlung bekannte Peter Norton soll angeblich zu dieser Zeit noch öffentlich verkündet haben, er glaube nicht an die Existenz von Viren. Das sei doch alles nur eine Legende, vergleichbar mit den Alligatoren in der öffentlichen Kanalisation New Yorks. John McAfee findet dagegen schnell heraus, dass der

unbedarfte Computer-Nutzer sehr wohl gerne an unberechenbare Gefahren in diesem ihm unverständlichen Kasten glaubt. 1988 baut er ein Wohnmobil mit Computern aus, tauft es "Virus Bug Buster" und lässt ein Team damit im Silicon Valley von Kunden zu Kunden fahren, um ihnen die Computer zu säubern. Rent to kill meets High Tech Ghost Busters - das sind Metaphern, die bei den Computernutzern besser ankommen als die leiseren Töne der Konkurrenz.

Zu diesem Zeitpunkt liegt die Zahl der existierenden Viren noch im zwei- bis dreistelligen Bereich. Tatsächlich in freier Wildbahn findet man davon noch sehr viel weniger. Dafür beginnen die Viren jetzt, die Medien zu infizieren. Neben den ersten Horror-Meldungen in diversen Tageszeitungen werden auch erstmals Viren im Source-Code publiziert und einer breiteren Öffentlichkeit zugänglich gemacht. Ralf Burger veröffentlicht 1987 im Data Becker Verlag "Das Große Computer-Virenbuch" mit dem Sourcecode einiger teilweise selbst programmierter Beispielviren. Ein Jahr später erscheint das Buch auch in englischer Übersetzung.

1990 zieht dann der Amerikaner Mark Ludwig mit seinem "Little Black Book of Computer Viruses" nach, das sogar samt einer Diskette mit Beispielviren ausgeliefert wird. Diese Veröffentlichtungen stoßen in der Antivirus-Community auf große Kritik. So wirft der bulgarische Antivirus-Experte Vesselin Bontchev den Autoren vor, Wissenschaftlichkeit nur als Schutzschild zu missbrauchen und Nachahmer zu provozieren. In Bezug auf Ludwigs Buch urteilt er:

"Alles, was wir dort zu sehen bekommen, ist ein Haufen unsinniger MS DOS-Viren, die kaum funktionieren."

Doch auch die einfachste Beschreibung des Phänomens reicht aus, um weltweit Computerfreaks zu begeistern. In der Septemberausgabe der deutschen Computerzeitschrift Chip erscheint ein Artikel von Chaos Computer Club-Mitglied Steffen Wernery unter dem Titel "Comuterviren - Die neue Gefahr?". Die bulgarische Computerzeitschrift "Computer za vas" druckt den Artikel ein halbes Jahr später übersetzt nach und legt damit den Grundstein für eine der vitalsten Virenprogrammierer-Szenen. Innerhalb von drei Jahren erreichen die bulgarischen Viren einen Anteil von zehn Prozent am Gesamt-Weltmarkt.

Das sozialistische Computerparadies

Aber warum gerade Bulgarien? Glaubt man den Überlieferungen des Antivirus-Experten Bontchev , dann ist Bulgarien Ende der Achziger so etwas wie das sozialistische Computerparadies. Das ZK der bulgarischen Kommunisten entscheidet Anfang des Jahrzehnts, mit der Produktion eigener Microcomputerserien zu beginnen, diese an den gesamten Ostblock zu liefern und so das Exportverbot des Westens zu unterlaufen. Allerdings entwickelt man keine völlig neuen Systeme, sondern spezialisiert sich auf das Klonen bereits existierender Modelle.

Zuerst werden mit dem IMKO und dem Pravetz 82 Systeme entwickelt, die möglichst perfekte Nachbildungen des Apple 2 darstellen. 1984 wird schließlich der Pravetz 8 entwickelt - ein 8bit-Mikrocomputer, der auch mit Microsofts DOS 3.3 arbeitet. Eine wichtige Voraussetzung für seinen Erfolg, denn um den Vorsprung des Westens aufzuholen, setzt man hier nicht auf das Entwickeln eigener Software. Statt dessen werden an diesen Maschinen ganze Generationen von Informatikern in Reverse Engineering ausgebildet. Ihre Studienaufgaben müssen ungefähr so ausgesehen haben: Nimm dir etwas Hardware aus dem Westen und bau es möglichst billig nach. Oder nimm dir Microsofts neueste DOS-Version, portier sie auf den Pravetz - aber lass bitte die Bugs weg.

Als dann Wernerys Chip-Artikel in bulgarischer Übersetzung erscheint, sind einige dieser Studenten sofort infiziert. Viren waren ihnen bis dahin unbekannt. Also besorgen sie sich den Vienna-Virus, der auch im Artikel beschrieben wird und verfahren damit so, wie sie es mit westlicher Software gewohnt sind: Disassemblieren, analysieren, optimieren. Weil es in Bulgarien auch keine Antivirus-Industrie gibt, mit der man das Katz- und Maus-Spiel spielen könnte, müssen sie die Katze gleich mit erfinden. Der Programmierer des Jan-

kee Doodle-Virus schafft sich deshalb sein eigenes Antiviren-Programm namens Vacsina. Daran probiert er seinen Virus aus, verstärkt den Schutz, verbessert den Virus, und so weiter. Einige seiner Viren verbinden sogar beide Techniken und deaktivierten andere Viren, die sich auf dem befallenen System befinden.

1990 entsteht dann in Sofia das erste Virus Exchange (vX) Bulletin Board - ein Mailboxsystem zum Austausch elektronischer Schädlinge, das mit einer Upload/Download-Ratio arbeitet. Wer sich Viren herunterladen will, muss dafür neue Viren hochladen. Weil bald alle bekannten Viren in das System eingespeist sind, müssen die User wohl oder übel neue programmieren. Bald wird die BBS mit ihren knapp 300 Nutzern weltweit als "virtuelle Virenuniversität" bekannt. Einer der aktivsten Studenten dieser Universität nennt sich Dark Avenger und ist ein höchst talentierter Programmierer aus Sofia. Anfang 1991 kündigt er an, einen Virus mit mehr als 4 000 000 Mutationsmöglichkeiten zu entwickeln.

Wir sind die Guten

Etwa zur gleichen Zeit kauft sich in den USA die Sozialarbeiterin Sarah Gordon ihren ersten PC. Nach kurzer Zeit erscheint auf ihrem Bildschirm ein kleiner, umherspringender Ball - ein sicheres Zeichen für den Ping-Pong-Virus. Gordons Interesse ist geweckt. Da sie schon früh Erfahrungen mit Mailboxen gesammelt hat, sucht sie im Fido-Netz nach mehr Informationen, und stößt dabei auf die Newsgroups der Virenprogrammierer-Szene.

Ein Name fällt ihr immer wieder auf: Dark Avenger. Er ist der Autor des gleichnamigen Viruses, der als extrem gefährlich gilt, weil er sich vor Virenscannern zu verbergen weiß, diese infiziert und damit auch jede überprüfte Datei befällt. Sarah Gordon versucht vergeblich, mit Dark Avenger Kontakt aufzunehmen. Dann probiert sie es mit einem Trick. In einer einschlägigen Newsgroup wünscht sie sich einen Virus, der ihren Name trägt. Wieder hört sie nichts von Dark Avenger. Bis im Januar 1992 sein lange angekündigter Mutations-Virus erscheint, ein Generator für polymorphe Viren mit abertausenden von Erscheinungsmöglichkeiten.

Erstaunlicherweise erkennen die meisten Antiviren-Programme Dark Avengers "Mutation Engine" schon nach wenigen Tagen. Doch offenbar waren einige Programmierer bei der Anpassung der Scanner zu eifrig. Neben Dark Avengers Mutationen werden jetzt plötzlich auch tausende von nicht infizierten Dateien als Viren erkannt. Die Antivirus-Industrie hat ein Problem. Und mitten in diesem Problem steht der Satz: "Wir widmen diesen kleinen Virus Sarah Gordon" - als wäre die Mutation Engine nichts weiter als eine nette Neujahrspostkarte.

In der Antivirus-Community heißt der Mutation Engine zunächst nur "Dedicated", und Sarah Gordon ist mit einem Mal bekannt wie ein bunter Hund. Doch das hält sie nicht davon ab, sich weiter mit dem Thema zu beschäftigen. Anfang der Neunziger sind die Fronten zwischen Virenprogrammieren und Antivirus-Forschern bereits deutlich verhärtet. Viele in der Antivirus-Industrie fordern bereits härtere Strafen für das Verbreiten von Computerviren und bemühten sich redlich, Virenprogrammierer per se als kriminell darzustellen.

Doch Sarah Gordon besitzt als Sozialarbeiterin andere Zugriffsmethoden:

"Ich stellte fest, dass es eine echte Diskrepanz zwischen dem, was die Antiviren-Leute über die "Bad Guys" sagten, und meinen Beobachtungen gab." (Aus Sarah Gordons FAQ

[Gordon beschließt, sich intensiver den "Bad Guys" zu widmen und erstmals systematisch deren Strukturen und Motivationen zu erforschen. Die Szene akzeptiert sie zwar, viele halten sie aber wiederum für eine von den "Bösen" - schließlich lässt sie sich ihre Forschungsarbeit von Firmen wie IBM und Symantec bezahlen. Sarah Gordon ironisiert diese wechselseitige Schwarzweißmalerei gerne. Ihre private Website firmiert konsequenterweise unter der Adresse www.badguys.org.

Aus Luis wird der Virusbuster

Wie Sarah Gordon kommt auch Luis Anfang der Neunziger zum ersten mal mit dem Ping-Pong-Virus in Kontakt. Unfreiwillig, versteht sich. "Mein einziges Interesse an dem Virus war, ihn zu killen", erklärt er dazu heute. Damals sammelt und tauscht er raubkopierte Programme. Auf der Suche nach ein paar neuen Spielen stößt er auf jemanden, der wie er Warez tauscht, aber auch ein paar ganz besondere Programme im Angebot hat. "Er zeigte mir, dass Viren eine interessante Sache sein können, wenn du mit ihnen umzugehen weißt. Er gab mir seine Virensammlung, ungefähr 40 oder so, und ich begann mit meinen eigenen Experimenten."

1994 entdeckt Virusbuster das Internet und damit die vX-Szene. Diese Szene hat im Netz seit etwa 1990 feste Strukturen gebildet. Von ganz elementarer Bedeutung sind dabei neben den Mailboxen zwei Internet-Dienste: Im August 1988 entwickelt der Finne Jarkko Oikarinen das Internet Relay Chat-Netzwerk (IRC). 1989 erfindet Tim Berners-Lee das World Wide Web, 1990 entwickelt er den ersten Web Browser. Das IRC ist noch heute für die vX-Szene das wichtigste Medium zum informellen Austausch. Das World Wide Web hat dabei geholfen, aus diesen informellen Strukturen feste Bünde zu schmieden. Man schließt sich zu einer Gruppe zusammen, gibt sich mit einer Website ein Gesicht, tauscht darüber Viren aus und gründet E-Zines. Im Juni 1991 erscheint die erste Ausgabe des 40hex-Magazins mit einer Mischung aus Viren-Sourcecode und Programmier-Anleitungen. Es dient zahlreichen Magazinen dieser Art als Vorbild.

Erste Verhaftungen

1992 ist ein schlechtes Jahr für die Antivirus-Industrie. Für den sechsten März kündigen einige Firmen Millionen von Computerausfällen durch den Michelangelo-Virus an. Betroffen sind jedoch letztendlich nur etwa 10 000 Rechner weltweit. Gleichzeitig tauchen in diesem Jahr die ersten wirklich einfach bedienbaren Virusgeneratoren auf, mit denen sich jeder Laie seinen eigenen Virus zusammenklicken kann.

Im Gegenzug verstärkt man den Druck auf die vX-Szene. 1993 kommt es zu den ersten Verhaftungen bei Mitgliedern der britischen Association of Really Cruel Viruses (ARCV). Das Antivirus-Lager feiert dies als Erfolg und hofft, dass ähnliche Aktionen weiteren Virenautoren das Leben schwer machen könnten. Doch bei genauerer Betrachtung des Falls stellt sich heraus, dass die ARCV-Mitglieder sich eines anderen Verbrechens schuldig gemacht haben: Sie benutzten Geräte zur Manipulation des Telefonnetzes (so genannte Brown Boxes), um mit kostenlosen Telefonaten Kontakt zu vX-Mailboxen in den Vereinigten Staaten aufzunehmen.

Zu einer ersten Verurteilung eines Virenprogrammierers kommt es erst 1995. Der 26-jährige Brite Chris Pile wird wegen der Verbreitung seiner SMEG-Viren und der eines manipulierten Antivirus-Programms zu 18 Monaten Gefängnis verurteilt. Viele Virenprogrammierer sind von dem Urteil gegen den Black Baron, wie er in der Szene heißt, schockiert. Vom Schreiben eigener Viren lassen sich dadurch aber nur die wenigsten abhalten. Doch viele überlegen es sich seitdem zweimal, ob sie einen Virus in die Wildnis entlassen. Die meisten Viren zirkulieren nur in der Szene, nur ein geringer Prozentsatz infiziert jemals die Rechner Unbeteiligter. Allein das Programmieren von Programmen, die sich selbst vervielfältigen, ist in den meisten Staaten aber nicht verboten.

Wer seine Viren dennoch in die Wildnis entlässt, bleibt gerne vollkommen anonym. "Virenprogrammier, die ihre Geschöpfe verbreiten, verbinden sich mit dem IRC über Proxy-Server", erklärt Luis eine der verbreiteteren Vorsichtsmaßnahmen. Er selbst hat nie einen Virus programmiert, würde seine eigenen Kreationen aber auch nicht in die Wildnis entlassen. Ähnlich geht es den meisten seiner Freunde von der 29a-Gruppe. In deren Policy heißt es:

"Wir programmieren Viren aus Spaß an der Sache, weil es unser Hobby ist, und nicht, um anderen zu schaden." Distanzieren möchten sie sich von Viren, die in der Wildnis auftauchen, jedoch nicht.

Windows 95: Neuanfang oder Terror?

Für Schlagzeilen sorgen meist nur die Viren, die tatsächlich Infektionen auslösen, unzählige Computersysteme außer Betrieb setzen oder sich besonders eigentümlich verbreiten. Wie etwa der Tremor-Virus, der im 1994 als erstes Programm seiner Art über das Fernsehen unters Volk gebracht wird. Zu dieser Zeit nutzt die deutsche Firma Channel Videodat die Austastlücke des Fernsehsenders Pro 7, um mit etwa 15kBit pro Sekunde Software an Käufer des Videodat-Decoders zu vertreiben. Im Mai 1994 findet auf diesem Weg auch eine infizierte Version des Dekompressions-Programms PkUnzip den Weg auf zahlreiche Festplatten. Drei Monate nach der Infektion werden tausende von Videodat-Usern damit konfrontiert, dass die Darstellung ihres Monitors wackelt, bevor sich der Rechner ganz aufhängt. In einigen Fällen meldete sich Tremor auch mit dem Front 242-Zitat "Moment of Terror is the Beginning of Life" zu Wort.

Neuanfang oder Terror - diese Frage stellt sich 1995 auch so manch ein Betatester von Windows 95. Microsoft verschickt in einigen Fällen Disketten, die mit dem Form-Virus infiziert sind. Doch diese peinliche Panne ist fast bedeutungslos gegen all die neuen Möglichkeiten, die das System Virenprogrammierern bietet. Anfang 1996 erscheint mit Bizatch der erste Windows95-spezifische Virus. Schon ein paar Monate vorher taucht mit Concept der erste Word-Macrovirus in freier Wildbahn auf. Beide legen den Grundstein für unzählige Nachfolger. 1996 kommt es zur ersten Windows-Virenepidemie.

Im selben Jahr gründen einige Virenprogrammierer um einen gewissen Mister Sandman die vX-Gruppe 29a, der wenig später auch Luis alias Virusbuster beitritt. Ihr Name ist die hexadezimale Darstellung des satanischen 666, und auch sonst lieben die 29a-Mitglieder kleine Zahlenspielereien. Am Freitag, dem 13. Dezember 1996 um 6 Uhr 66 morgens erscheint die erste Ausgabe ihres Magazins, mit dem die Gruppe sozusagen offiziell ihre Gründung begeht. Es enthält Programmieranleitungen, Viren-Sourcecode und -analysen und ein Dutzend Viren als ausführbare Dateien, sowie Tipps zum Umgehen von Antivirus-Schutzmechanismen, die hier "Klingon Tech" genannt werden.

Dazu liefern die 29a-Mitglieder einen eigenen Textbetrachter, der als Bildschirmschoner die Payload-Ausgabe des LSD-Virus verwendet. Solche Gimmicks wiederholen sich in den nächsten Ausgaben. Nummer zwei des 29a-Magazins erscheint mit einem animierten Intro, wie man es von Veröffentlichungen der Demo-Scene kennt.

Intern ist die Gruppe gewissermaßen basisdemokratisch organisiert. Es gibt keinen Anführer, lediglich für eine neue Ausgabe ihres Magazins wird eine Art Redakteur bestimmt. Ganz auf die Gruppe ausgerichtet sind auch die Initationsregeln: "Wenn jemand Mitglied bei 29a werden will, muss er uns seine Artikel und Viren schicken, damit wir die Qualität seiner Arbeit beurteilen können. Die Mitglieder überprüfen dann sein Material und auch ihn als Person. Wenn alle dafür sind, kann er Mitglied werden. Bei nur einer Gegenstimme wird er nicht Mitglied", erklärt Luis. Andere Entscheidungen werden per Mehrheitsbeschluss gefasst.

Nach Schätzungen von Sarah Gordon gibt es derzeit rund 20 beständig aktive Gruppen wie 29a. Daneben existieren noch eine ganze Zahl von Gruppierungen, die nur kurz auf der Bildfläche erscheinen, sich aber sofort wieder auflösen oder mit einer anderen Gruppe verschmelzen. 29a jedoch beweist Kontinuität - zwar veröffentlichen sie gerade mal ein Magazin pro Jahr, dafür gehen auf das Konto der Gruppenmitglieder einige der innovativsten und kreativsten Viren der letzten Jahre.

In der zweiten Ausgabe ihres Magazins erscheint mit Esperanto der erste Virus, der sowohl Windows- als auch Macintosh-Rechner infizieren kann. An jedem 26. Juli - dem Tag, an dem 1887 das erste Buch über die Kunstsprache Esperanto erschien - verkündet der Virus:

Never mind your culture / Ne gravas via kulturo, Esperanto will go beyond it / Esperanto preterpasos gxin; never mind the differences / ne gravas la diferencoj, Esperanto will overcome them / Esperanto superos ilin.

Never mind your processor / Ne gravas via procesoro, Esperanto will work in it / Esperanto funkcios sub gxi; never mind your platform / Ne gravas via platformo, Esperanto will infect it / Esperanto infektos gxin.

Von diesem kleinen Sprachkurs abgesehen richtet der von Mr. Sandman programmierte Virus keinen weiteren Schaden an.

Viren: Politik, Forschung, pubertäter Spaß?

Im gleichen Magazin erscheint auch der Anti-ETA-Virus von Griyo, mit dem die Gruppe kollektiv gegen den baskischen Terrorismus Stellung bezieht. Es ist nicht der erste Virus mit einer politischen Botschaft. Aber taugen Viren als Mittel politischer Meinungsäußerung? Heute sehen die 29a-Mitglieder dies selbst eher skeptisch und tun es als eine Art Jugendsünde ab. Griyo hat sich als Autor des Viruses mittlerweile von dieser Aktion distanziert, und Luis erklärt:

"Das ist eher eine persönliche Leidenschaft einiger Mitglieder der Szene. Die Mehrheit der Virenprogrammierer vermischt Politik und Viren nicht. Ich bezweifle sogar, dass die große Mehrheit der Virenprogrammierer in der Szene sich überhaupt um so etwas kümmert."

Auch den Versuch, das Programmieren von Viren selbst als politisch, weil ja irgendwie diffus gegen das System gerichtet zu begreifen, blockt er sofort als unzulässige Projektion ab: "Ich sehe im Programmieren eines Virus keinen politischen Akt."

Aber warum machen sie es dann? Mit dieser Frage beschäftigt sich auch Sarah Gordon, seit die die Szene als ihr Forschungsobjekt entdeckt hat. Eine eindeutige Antwort darauf kann sie bis heute nicht geben, denn Virenprogrammierer "sind so verschieden wie ihre Viren", so Gordon. Einige handeln aus Spaß an der Sache, andere wollen es in der Szene zu etwas bringen oder genießen es, wenn Antivirus-Firmen ihre Programme rezensieren. Wieder andere üben einfach ihre Programmierkenntnisse an diesen Kreationen, oder sie genießen den Kitzel am Illegalen - etwa, wenn sie eine ihrer Kreationen in die Wildnis entlassen. Perikles, ein mit Luis befreundeter Virensammler, begründet seine Leidenschaft im Gespräch scherzhaft so:

"Vielleicht bin ich an Viren interessiert, weil ich einen Entomologen-Komplex habe, wie Jünger. Jedenfalls finde ich es interessant, die Schwächen eines Betriebssystems zu erforschen."

Dieses Forschungsmotiv taucht immer wieder in der Szene auf. Die 29a-Homepage nennt sich "29a Labs", und deren Mitglied Griyo betreibt nebenbei noch seine private Website unter dem Namen "BiO.net - Virus Research Labs". Antivirus-Forscher werden dagegen nicht müde, zu betonen, dass ohne eine entsprechende Ethik, einen verantwortungsvollen Umgang mit dem Virencode, keine Forschung möglich ist. Doch die vX-Szene ignoriert solche Belehrungen forsch.

Gefängnis oder Job-Offerte?

Am 26. April 1998 entlässt der taiwanesische Wehrdienstleistende Chen Ing-hau seinen CIH-Virus in die Wildnis. Schon nach einer Woche gelangt der Virus über das Internet nach Europa und in die USA, wo er versehentlich mit Promotion-Downloads und kostenlosen CD-ROMs vertrieben wird. CIH wird damit kurzzeitig zu einem der meistverbreiteten Viren, und zu einem der gefährlichsten noch dazu: Am 26. April 1999 löscht er Daten auf dem Wirtscomputer. Auf einigen wenigen Rechnern gelingt es ihm sogar, das BIOS zu überschreiben. Chen Ing-hau wird nach Enthüllung seiner Identität kurzzeitig verhaftet, doch da niemand ihn in Taiwan verklagt, bald ohne Anklage wieder freigelassen. Wenig später wird er vom taiwanesischen Linux-Distributor Wahoo als Sicherheits-Experten eingestellt.

Die Antivirus-Industrie reagiert empört. Ein Jahr später allerdings wird sein Virus wieder aktiv. Diesmal findet sich ein taiwanesischer Student als Kläger, und Chen wird zu drei Jahren Gefängnis verurteilt. Ein Vetreter der Firma Sophos Anti-Virus erklärt: "Dies ist ein deutliches Signal an Virenprogrammierer, dass sie der Strafe für ihre Handlungen nicht entkommen werden."

Doch das Verhältnis zwischen Antivirus-Experten und der vX-Szene wird nicht allein von solch harten Law and Order-Töne bestimmt. Sarah Gordon beispielsweise beschreibt die 29a-Mitglieder als "sehr nette Leute. Es hat mir immer Spaß gemacht, mich mit ihnen auszutauschen." Ganz ohne Austausch kommen sie und ihre Kollegen aber auch gar nicht aus, wenn sie wollen, dass ihre Antiviren-Scanprogramme neue Schädlinge möglichst frühzeitig erkennen.

Oft bekommen Antivirus-Programmierer diese direkt von den Autoren zugeschickt, die sich über eine kompetente Analyse ihrer Programmierleistung immer freuen. Luis berichtet außerdem, dass er seit Jahren mit Antivirus-Programmierern in Kontakt steht. "Sie benutzen mich als Quelle für ihre Arbeit und ich benutze sie als Quelle für meine Sammlung." Glaubt man ihm, arbeiten in einigen dieser Firmen ehemalige Virenprogrammierer und sogar aktive Mitglieder der Szene. Ob er sich selbst vorstellen könnte, irgendwann bei solch einer Firma unterzukommen? "Irgendwann? Wenn sie gut genug zahlen schon morgen!"

Überlaufangebote werden allerdings auch an die andere Seite gemacht. Als der tschechische 29a-Programmierer Benny seinen Win98.Millenium-Virus entwickelt, gelangt eine Beta-Version auf unbekannte Weise in die Hände des rumänischen Antivirus-Spezialisten Adrian Marinescu. Marinescu veröffentlicht eine Analyse des Schädlings, und Benny ist voll des Lobs: "Gute Arbeit, Adrian!" Spaßeshalber fordert er ihn in einem Szene-Magazin auf: "Fuck of AV, join 29a!" (BadByte Magazine Issue 3)

Adrian Marinescu gehört zu einer jungen Generation von Antivirus-Experten, die schon optisch nicht mehr viel mit den John McAfees und Peter Nortons dieser Welt gemeinsam hat. Er trägt einen Kinnbart, schlabbrige Klamotten und bezeichnet Biertrinken als eines seiner großen Hobbys. Bennys Angebot lehnt er trotzdem dankend ab:

"Ich würde nie auf die andere Seite gehen. Für mich ist es kein Spaß, anderen Usern zu schaden. Einige Virenprogrammierer erklären, dass sie nur lehrreiche Viren schreiben, die niemandem schaden. Das ist nicht wahr. Schon weil sie sich selbst vervielfältigen, richten sie Schaden an."

Er selbst gehe Virenprogrammierern nicht aus dem Weg, sondern versuche sie davon zu überzeugen, ihr Hobby aufzugeben. Schließlich weiß er durch seine tägliche Arbeit: "Einige von ihnen sind begabte Programmierer."

Primitive Makros und autonome Mutanten

Aber zur Umkehr bewegen konnte er noch keinen. Und so geht das Katz- und Mausspiel weiter. Am Freitag, dem 26. März 1999 taucht in der Newsgroup alt.sex erstmals ein Word-Makrovirus namens Melissa auf. Innerhalb weniger Stunden verbreitet er sich über Microsofts Outlook E-Mail-Client in ganz Nordamerika. Das FBI beginnt mit der Suche nach dem Melissa-Autor. Als am Montag dem 29.März in zahlreichen Büros die Desktop-PCs wieder eingeschaltet werden, beschleunigt sich die Melissa-Verbreitung exponentiell. Mehr als 100 000 PCs werden angeblich an diesem Tag infiziert. Am ersten April wird David L. Smith als mutmaßlicher Melissa-Autor festgenommen. Zu seinem Verhängnis wird eine geklaute AOL-Adresse, mit der er den Virus in die Newsgroup eingespeist hat.

Melissa überrascht Antivirus-Hersteller wie Virenprogrammierer gleichermaßen. "Es erwischte uns mit heruntergelassenen Hosen", erklärt Network Associates-Forscher John Bloodworth ein Jahr später auf der Virus Bulletin Conference. Durch die Kombination von Word-Macros und Fortpflanzung per E-Mail verbreitet sich der Virus so schnell, dass kaum ein PC ausreichend dagegen geschützt, kaum ein Nutzer darauf vorbereitet ist.

Antiviren-Firmen müssen beobachten, wie tausende von Computerbesitzern sich durch das Öffnen des Melissa-Attachments ins Verderben klicken. Doch auch die vX-Szene hat in den folgenden Wochen unter Melissa zu leiden. Das FBI besucht verscheidene ISPs und Webmaster von vX-Websites. Einige löschen daraufhin vorsichtshalber ihr komplettes Angebot. Auf der Seite des mutmaßlichen Melissa-Autors prangt heute nur noch ein Logo der Antivirus-Software AVP.

Für Schlagzeilen sorgen auch in den kommenden Monaten Melissa-ähnliche Makroviren wie etwa der ILoveYou-Virus. Doch aus Sicht der Szene sind diese Geschöpfe eher primitiv. Hier bastelt man lieber an möglichst schwer zu entdeckenden Viren wie dem Marburg-Virus oder dem HPS-Virus, die beide auf das Konto von 29a-Mitglied Griyo gehen und versehentlich von PC-Spielemagazinen verbreitet werden. Beide Viren benutzen polymorphe Techniken, um Virenscannern zu entgehen. Mittels zufallsbasierter Verschlüsselung verstecken sie sich in immer neuem Code, so dass sie über einfachen Codeabgleich nicht mehr auffindbar sind.

Doch damit nicht genug: Noch komplexer wird die Angelegenheit, wenn sich zwei solcher Viren gegenseitig infizieren. Die Chancen, sie dann noch zu entdecken, sinken stark. Wird doch einer gefunden, kann dies noch katastrophalere Folgen haben. Wenn das Antivirenprogramm ihn entfernt und dabei den Code des unentdeckten Virus modifiziert, entsteht unter Umständen als autonome Mutation ein völlig neuer Virus - einer, der nicht entdeckt werden kann, der keinen Autor hat.

Viren im Reich der Pinguine

Im Februar 1997 erscheint dann mit Lin-Bliss der erste Linux-Virus. Viele haben bis dahin das Open Source-Betriebssystem für immun gehalten, doch sie hatten offenbar noch nie etwas von Fred Cohen gehört. Schließlich hatte der schon 13 Jahre vorher festgestellt: Kein System ist sicher. Der einsetzende Linux-Boom verschärft das Problem noch. Gerade Linux-Anfänger, die sich die ganze Zeit als Systemadministrator (Root) einloggen, sind für Viren wie Lin.Bliss besonders anfällig. Im März 2001 gelingt 29a-Mitglied Benny schließlich etwas außergewöhnliches. Er veröffentlicht den ersten Virus, der sowohl Windows- als auch Linux-Rechner infizieren kann.

Viren wie dieser bieten Antivirus-Softwareherstellern zwar die Möglichkeit, ihren Markt auf neues Terrain auszudehnen, bergen aber auch neue Konflikte. Die Linux-Gemeinde ist eine völlig andere Informationspolitik gewöhnt als AV-Firmen. Taucht unter Linux eine Sicherheitslücke auf, so wird dies auf einschlägigen Mailinglisten und in Weblogs wie Slashdot.org publiziert, damit Administratoren die Lücke auf ihrem System möglichst schnell schließen können. Quellcode und detaillierte Fehlerbeschreibungen gehören dabei geradezu zum guten Ton.

Für Antivirus-Experten ist dagegen jede Publikation eines Viren-Sourcecodes unmoralisch. Sie tauschen Viren nur in geschlossenen Zirkeln aus und veröffentlichen lediglich Analysen ohne Source Code.

In der Sprache der Open Source-Gemeinde heißt solch eine Praxis verächtlich "Security by Obscurity". AV-Forscher argumentieren dagegen, das man einen Virus nicht mit einer Sicherheitslücke in einer Firewall vergleichen kann. Diese könne mit den regelmäßig veröffentlichten Bug-Fixes schnell gestopft werden, danach sei das System sicher. Ein Virus müsse dagegen nur minimal verändert werden, um wieder ein Sicherheitsrisiko darzustellen. Der Moderator der Bugtraq-Mailingliste Elias Levy will dies nicht gelten lassen: "Darin liegt das Problem der ganzen Antivirus-Community. Der Hersteller hat niemals einen Bugfix veröffentlicht. Ihr seid so dadurch konditioniert, dass der Hersteller nie einen Bugfix veröffentlicht hat, dass ihr glaubt, es gibt keinen Bugfix."

Ein RFC für Netzwerk-Viren

Der Hersteller, von dem Levy hier spricht, ist natürlich Microsoft. Und auch wenn sich die Zahl der Linux-Viren sicher noch erhöhen wird, auch wenn mittlerweile schon Viren für Palm Pilots aufgetaucht sind und es bis zum ersten Playstation2-Virus wohl nur noch eine Frage der Zeit ist, steht doch fest: Windows bleibt das Hauptbetätigungsfeld der Virenprogrammierer. Schon jetzt danken sie in ihren Publikationen gerne mal spaßeshalber Microsoft für die vielen Dinge, die ihnen diese Firma bisher ermöglicht hat.

Luis ist sich sicher, dass sich daran auch in Zukunft nichts ändern wird: " Die interessantesten Trends werden weiterhin die sein, die mit Microsoft zusammenhängen. Viren werden, wie schon bisher, sehr davon abhängig sein, was Microsoft tun wird." Ein weiterer Trend liegt im Netz. Neben IRC-Würmern und Makroviren der zweiten Generation scheinen sich selbst updatende Viren der letzte Schrei unter Virus-Autoren zu sein. Erfunden hat diese Funktion ironischerweise die Antivirus-Industrie, um Kunden regelmäßig mit neuen Virendefinitionen zu versorgen.

Doch schnell haben Virenprogrammierer entdeckt, dass sich auch ihre Geschöpfe neue Komponenten übers Netz besorgen können. Im 29a-Magazin vier veröffentlicht ein Programmierer namens Venca erstmals einen Virus, der sich zusätzliche Module - Venca nennt sie "Plug-Ins" - über eine Webseite herunterladen kann. Eine ähnliche Technik nutzt auch der MTX-Virus, der im Herbst 2000 große Verbreitung findet.

Noch einen Schritt weiter geht der ebenfalls von Venca programmierte Hybris-Wurm: Für ihn existieren bis zu 32 Plug-Ins, die verschlüsselt von einer Website heruntergeladen werden können. Diese ist mittlerweile geschlossen worden, doch Hybris ist damit nicht aus dem Rennen. Zusätzlich kann er sich seine Plug-Ins auch über die Newsgroup alt.comp.virus besorgen - ein Diskussionsforum, das auch von Antivirus-Experten genutzt wird. Andere Viren und Würmer updaten sich selbst über FTP-Server oder loggen sich automatisch in einen bestimmten IRC-Channel, um weitere "Fernwartungskommandos" abzuwarten.

Doch das ist erst der Anfang. Längst feilen die Virenprogrammierer an komplexeren Netzwerk-Nutzungsmöglichkeiten. Ein Testfall dafür könnte der Gnutella-Wurm Gspot von 29a-Mitglied Mandragore gewesen sein. Er breitet sich im Juni 2000 unter Nutzern des Napster-ähnlichen Filesharing-Netzwerks aus, indem er Suchanfragen auswertet und diese pauschal positiv beantwortet. Sucht jemand etwa nach Photoshop, gibt Gspot sich als Photoshop.exe aus. Interessanter als dieser einfache Trick ist jedoch das Netzwerk, dessen sich der Wurm bedient. Was, wenn Viren ein eigenes Peer-to- Peer-Netzwerk aufbauen würden, um über infizierte Computer unbemerkt Informationen und Updates auszutauschen? Was wie Zukunftsmusik klingt, ist vielleicht gar nicht mehr so weit von der Realität entfernt. Im 29a-Magazin Nummer fünf beschreibt ein gewisser Bumblebee ein Konzept, mit dem sich Viren selbst verschlüsselt über eine eigene Netzwerkstruktur updaten können. Scherzhaft beschließt er seinen Artikel mit der Aufforderung: "Let's start our own RFC!"

Wem das einen kalten Schauer über den Rücken jagt, der sollte sich lieber an die Zukunftsperspektive eines Experten wie Adrian Marinescu halten: "Internetbasierte, selbst-updatende, metamorphe Viren werden wir in den nächsten Jahren immer häufiger begegnen. Das sind die Techniken der Zukunft - aber ich wette, dass die in der Wildnis vorkommenden Viren im nächsten Jahr genau so albern sein werden wie etwa der ILoveYou-Virus."