DAS KLEINE KASPERSKY-VIRENLEXIKON

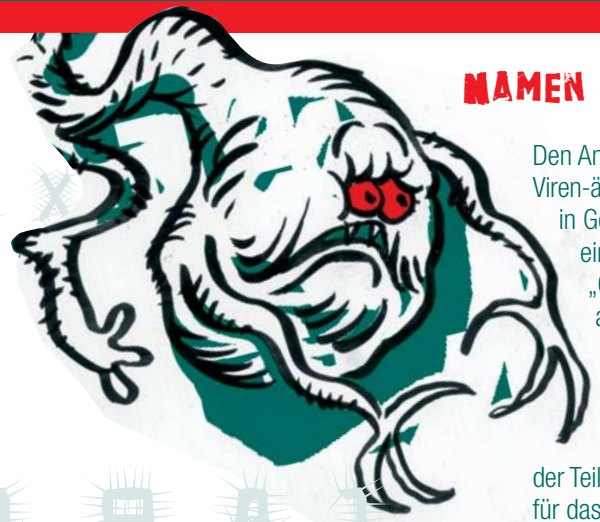
KASPERSKY lab

INHALTSVERZEICHNIS

VORWORT

Viren, Würmer, Trojanische Pferde, Rootkits – das Internet hat nicht nur für schnelle E-Mails und Videoclips a la YouTube gesorgt. Auch die Bedrohungen sind vielfältiger und vor allem gefährlicher geworden. Dabei hatte alles so harmlos angefangen, die ersten Entwicklungen mit Viren, die damals noch nicht einmal diesen Namen trugen, gehen bis in die graue Vorzeit der Computertechnik zurück. Die Programmierer hatten hehre Ziele, wollten sich selbst reparierende Software schaffen, Programme, die sich ständig verbesserten. Heute ist davon kaum etwas übrig geblieben, Viren sind im besten Fall lästige Begleiterscheinungen der Arbeit mit dem Computer, im schlimmsten Fall gefährden sie Daten und Bankkonten.

Sicher, Antivirus-Programme gehören heute zur Standardausstattung eines Büro- und Heim-PC. In vielen Fällen schützen sie vor Infektionen und blockieren Angriffe. Doch Viren-Autoren und die Entwickler von Schutz-Software liefern sich seit Jahren ein Rennen, das immer schneller wird, der Vorsprung jeder Seite immer kürzer. Letztendlich gibt es keine absolute Sicherheit, jedenfalls nicht bei einem Computer, der Verbindungen mit der Außenwelt herstellt. Doch aktuelle Antivirus-Software, das Einspielen von Patches für Betriebssystem und Anwendungen und – besonders wichtig – gesunder Menschenverstand sowie eine Portion Misstrauen gegenüber verdächtigen E-Mails und Webseiten sorgen auch in Zukunft für einen infektionsfreien PC.



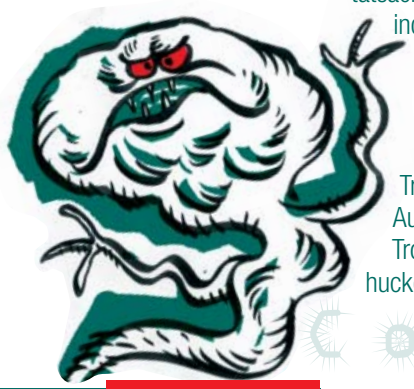
NAMEN SIND SCHALL UND RAUCH

Den Anfang machten Viren, dann kamen die Würmer. Doch als die ersten Viren-ähnlichen Programme entwickelt wurden, war dieser Name noch nicht in Gebrauch. Erst 1981 verwendet Professor Leonard M. Adleman in einem Gespräch mit Fred Cohen zum ersten Mal den Begriff „Computervirus“. Drei Jahre später liefert Cohen seine Doktorarbeit ab, Titel: „Computer Viruses - Theory and Experiments“. Zum ersten Mal wird definiert, was ein Computervirus ist und welche Eigenschaften er hat. Cohen beschreibt einen Virus als „ein sich selbst vervielfältigendes Programm, das andere Programme infizieren kann, indem es ihnen seinen eigenen Code anhängt“. Brisant ist der Teil mit den „Experiments“. Darin stellt Cohen ein funktionierendes Virus für das Betriebssystem UNIX vor, er gerät deshalb in die Kritik.

„Es gibt nur einen sicheren Computer. Er ist nicht vernetzt und befindet sich in einem Safe 20 Meter unter der Erde an einem geheimen Ort...und selbst da habe ich meine Zweifel.“

Dennis Hyges, FBI

Heute wird der Begriff „Virus“ meist für alle Arten Schadprogramme benutzt, tatsächlich gibt es aber genaue Abgrenzungen. Ein Virus verbreitet sich, indem es sich in noch nicht infizierte Dateien kopiert und so anpasst, dass es selbst ausgeführt wird, sobald man das Wirtsprogramm startet. Ein Wurm wartet hingegen nicht passiv darauf, aufgerufen zu werden sondern betreibt aktiv seine Verbreitung. Würmer nutzen dazu meist Sicherheitslücken in Software und Betriebssystem. Trojaner, die dritte große Gruppe, stellen sich zum Zeitpunkt der Ausführung als etwas anderes dar, als sie in Wirklichkeit sind. Ein Trojaner repliziert oder kopiert sich nicht selbst und wird daher meist huckepack mit einem Wurm oder Virus kombiniert.



ANFÄNGE UND FRÜHE KONZEPTE

Die Kreidezeit der Computertechnik war eine weitgehend ideale Periode. Computer waren mächtige Ungetüme, die nur Wissenschaftlern und sehr großen Firmen zur Verfügung standen. Die Rechenleistung konnte zwar nicht mit der eines aktuellen Videorekorders mithalten, dennoch wurden hier die Grundsteine für die Computertechnik gelegt, wie wir sie heute kennen. Viele Ideen kamen über das Papierstadium nicht hinaus. So hatte John von Neumann (eigentlich Janos Lajos Neumann) schon Mitte der vierziger Jahre theoretische Vorarbeiten zu sich selbst reproduzierenden Programmen geleistet, auch wenn an die Umsetzung zu der Zeit noch nicht zu denken war. 1959 veröffentlichte der britische Mathematiker Lionel Penrose einen Artikel über automatische Selbst-Replizierung in der Zeitschrift „Scientific American". Seine „virtuellen" Geschöpfe konnten sich vervielfältigen, verändern und andere Programme angreifen. Kurz danach verwirklichte Frederick G. Stahl Penrose' Modell auf einem IBM 650 Computer.

Irren ist menschlich
Marcus Tullius Cicero

Von Viren und Würmern konnte man damals noch nicht sprechen, der Begriff selbst tauchte erst viel später auf. Den Entwicklern ging es um Konzepte, sie versuchten schon damals, der Maschine so etwas wie Intelligenz einzuhauchen. Dazu gehörte 1962 auch „Darwin" der Vorläufer des Spiels „Core Wars". Darwin wurde von drei Ingenieuren der Bell Telephone Laboratories entwickelt, Victor Vyssotsky, Doug McIlroy und Robert Morris Senior. Vor allem Robert Morris spielt in der weiteren Geschichte der Computerviren noch eine wichtige Rolle. Darwin, und sein Nachfolger Core Wars, fand auf einem virtuellen Schlachtfeld im Speicher des Computers statt. Die Mitspieler entwarfen simple Programme mit einer vereinfachten Programmiersprache. Die Programme konnten sich vervielfältigen, andere Programme aufspüren und vernichten. Ziel war es, das Schlachtfeld unter Kontrolle zu bringen.

Langsam näherten sich die Ideen und Konzepte dem an, was heute als Virus bekannt ist. Veith Risak veröffentlichte 1972 einen Artikel über selbstreproduzierende Automaten. Das darin beschriebene Programm hat bereits sehr deutliche Anklänge an moderne Viren. Es wird kurz danach auf einem Großrechner von Siemens programmiert und funktioniert problemlos.

„Irren ist menschlich, aber damit die Dinge richtig schief laufen, braucht man einen Computer"
Paul Ehrlich

MORRIS

Am 2. November 1988 erlebt das damals als Internet bekannte Computernetz seine erste Epidemie. Robert Tappan Morris, der Sohn von Robert Morris Senior, startet auf einem Vax Computer von Digital Equipiment seinen „Morris Worm“. Das Programm hat nur eine Aufgabe, sich so schnell als möglich auf so viele Computer wie möglich zu verteilen. Danach sollte es einfach nur im Speicher laufen, einen mikroskopisch kleinen Teil der Rechenzeit belegen und nichts tun. Den ersten Teil seiner Aufgabe erledigt der Wurm perfekt, schon nach drei Stunden sind mehrere Tausend Computer in ganz Amerika infiziert. Doch Programmfehler sorgen für eine böse Überraschung – der Wurm erzeugt auf jedem Computer immer neue Kopien von sich selbst, bald sind die Rechner nur noch damit beschäftigt den Wurm auszuführen.

Am Ende waren geschätzte 6000 Computer infiziert, das entsprach zur damaligen Zeit mehr als 10 Prozent des gesamten Internets. Sie mussten vom Netz genommen und aufwändig von der Infektion befreit werden. Die verursachten Kosten ließen sich nie genau festlegen, Schätzungen schwanken zwischen 10 und 100 Millionen US-Dollar. Morris wurde zu drei Jahren Haft auf Bewährung, 400 Stunden Sozialdienst und 10.050 Dollar Strafe verurteilt. Er ist heute Professor am renommierten Massachussets Institute of Technology (MIT), dem gleichen Ort, an dem er den Wurm startete. Als unmittelbare Folge wurde im Dezember 1988 das Computer Emergency Response Team (CERT) ins Leben gerufen, eine herstellerunabhängige Institution, die Gegenmaßnahmen gegen groß angelegte Attacken koordinieren soll.

Der Begriff „Wurm“ für eine Software, die sich selbstständig vervielfältigt und dabei bestimmte Aufgaben ausführt, stammt vom Science-Fiction-Autor John Brunner. In seinem Roman „Der Schockwellenreiter“ nutzt der Protagonist einen solchen Wurm (Tape-Worm) um sich Informationen zu verschaffen und seine Spuren in einem weltweiten Netzwerk, ähnlich dem Internet, zu verschleiern.

CREEPER

Unschuldige Zeiten: Der Creeper-Virus war nicht nur harmlos, er teilte auch der Welt mit, dass er sich auf einem Computer eingenistet hatte. Anfang der 70er Jahre für das Betriebssystem Tenex programmiert, konnte sich Creeper über Modems von Computer zu Computer bewegen. Dort erschien dann die Zeile: „I'M THE CREEPER, CATCH ME IF YOU CAN“.

Der Urheber wurde nie zweifelsfrei geklärt, die meisten Quellen geben Bob Thomas als Autor an. Das Ganze war nur als Experiment gedacht, doch, ganz im Sinne des Zauberlehrlings, der die Geister nicht mehr los wird, die er gerufen hat, geriet Creeper außer Kontrolle und pflanzte sich munter fort. Schaden entstand dabei keiner, trotzdem setzte sich Thomas auf seinen wissenschaftlichen Hosenboden und programmierte „Reaper“. Das Programm pflanzte sich ebenfalls automatisch fort und löschte Creeper wo immer es das Virus-Programm finden konnte. Somit könnte man „Reaper“ als erstes Antivirus-Programm der Welt bezeichnen.

ELK

Jugend forscht, leider manchmal in die falsche Richtung. 1982 ist Richard Skrenta 15, als er Elk programmiert, einen Virus für die damals extrem populären Apple II Heimcomputer. Elk, manchmal auch Elk Cloner genannt, hat die fragwürdige Ehre, der erste Virus zu sein, der sich „in-the-wild“ verbreitet, also auch außerhalb einer akademischen oder Forschungseinrichtung auftaucht. Auf Elk angesprochen sagte Skrenta: „Es war der idiotischste Hack, den ich je gemacht habe, aber er hat mir die meiste Aufmerksamkeit eingebracht.“ Geschadet hat es ihm nicht, heute ist Skrenta CEO beim erfolgreichen News-Aggregator Topix.net.

> Eine Personal Firewall bietet Schutz vor klassischen Angriffen. Was hat man unter "klassischen Angriffen" zu verstehen? Seltsam angezogene Fremde rollen ein riesiges Holzpferd vor Deine Haustür?
>
> IRC, Autor unbekannt

BRAIN

Globalisierung macht auch vor Viren nicht halt. 1986 programmieren zwei Brüder in Pakistan den „Brain“-Virus (auch Pakistani flu), den ersten Virus für IBM-PCs. Er ist harmlos, verändert nur den Namen der befallenen Diskette in „Brain“ und pflanzt sich auf noch nicht infizierte Disketten fort. Basit Farooq Alvi und sein Bruder Amjad bringen sogar ihren Namen und die korrekte Adresse im Programmcode unter. Eigentlich möchten die beiden, die zu der Zeit bei einem Softwarehersteller arbeiten, nur herausfinden, wie schlimm es um Raubkopien in Pakistan bestellt ist. Die Antwort ist eindeutig – sehr schlimm. Binnen weniger Monate reist „Brain“ um die Welt, er wird zur ersten globalen Epidemie. Brain gilt als erster „Stealth“-Virus der Welt, der seine Anwesenheit aktiv verbergen konnte. Versuchte der Computer lesend auf den Sektor zuzugreifen, auf dem sich der Virus eingenistet hatte, zeigte Brain den ursprünglichen Inhalt des Sektors an.

VIENNA

Schwarzer Peter für Virenautoren: 1988 zieht der Vienna-Virus um die Welt und infiziert Dateien mit der Endung „com“. Mittlerweile ist ein Computervirus für Medien und Unternehmen interessant, in den Zeitungen wird über „Vienna“ berichtet. Franz Swoboda, der erste, der auf den Virus aufmerksam macht, gerät unter Verdacht. Er gibt an, dass er den Virus von Ralf Burger erhalten hat, einem Mitglied des Chaos Computer Club (CCC). Burger ist empört und streitet das ab. Seinen Angaben nach hat er den Virus von Swoboda erhalten. Es wurde nie geklärt, wer tatsächlich der Autor ist. Vienna selbst ist harmlos, er hat keine Aufgabe, außer sich zu verbreiten. Geschichte schreibt der Virus aus einem anderen Grund. Bernt Fix, der eine Kopie des Virus erhält, schreibt ein Programm um Vienna zu neutralisieren. Es gilt als erstes erfolgreiches Antivirus-Programm für IBM-PCs.

CASCADE

Cascade läutet 1988 die zweite Virengeneration ein. Zum ersten Mal ist ein Virus speicherresident, bleibt also nach dem ersten Start im Arbeitsspeicher des Computers aktiv und infiziert automatisch neue "com"-Dateien. Außerdem verschlüsselt sich Cascade selbst, so ist er schwieriger zu entdecken, weil die damals üblichen Mustervergleiche nicht mehr greifen. Cascade ist auf den ersten Blick durchaus humorvoll – ab und an lässt er die Buchstaben auf dem Bildschirm bröckeln und bröseln, sie sammeln sich als kleine Häufchen am unteren Bildschirmrand. Dann gibt es allerdings eine böse Überraschung, Cascade löscht Sektoren auf Datenträgern. IBM nahm den Virus zum Anlass ein eigenes Anti-Viren Programm zu entwickeln. Und noch jemand wurde durch Cascade zum Anti-Viren Profi: Cascade war der erste Virus, den Eugene Kaspersky analysierte.

PEACH

Die Viren schlagen zurück. 1992 setzt sich zumindest in einigen Bereichen der Industrie das Wissen um die Notwendigkeit von Antivirus-Programmen durch. Prompt reagieren die Autoren der lästigen Biester: Peach erkennt, wenn Central Points Change Inspector auf dem PC installiert ist und löscht dessen Datenbank. Kann es die Datenbank nicht finden, erstellt es kurzerhand eine neue. In beiden Fällen wird die Antivirus-Software außer Gefecht gesetzt.

MICHELANGELO

Und dann kam Michelangelo...1992 löste dieser Virus eine noch nie vorher da gewesen Medienhysterie aus. Man könnte sagen, mit Michelangelo waren Viren im Medienzeitalter angekommen. Benannt wurde der Virus nach dem Universalgenie des Mittelalters weil er am 6. März, dem Geburtstag Michelangelos, aktiv werden und schlimme Schäden anrichten sollte. Michelangelo war schon 1991 entdeckt worden, aber erst im Januar 1992 begann der Rummel. Zwei Computerhersteller veröffentlichten Pressemitteilungen, dass sie versehentlich mehrere Hundert, mit dem Virus infizierte Disketten, ausgeliefert hatten. Nachrichtenagenturen und Tageszeitungen begannen über den Virus zu berichten und plötzlich überschlugen sich die Reporter mit immer noch alarmierenderen Zahlen über die zu erwartenden Schäden. Fünf Millionen Computer, zu der Zeit eine enorme Menge, sollte betroffen sein, die Schäden in die Millionen gehen. Michelangelo war auch in der Tat bösartig. Er hielt sich nach der Infektion unsichtbar im Hintergrund, überschrieb aber am 6. März den Boot-Sektor und verschiedene Systemdateien auf der Festplatte. Damit startete der Computer nicht mehr. Ob es an den Warnungen lag, oder an der völlig überschätzten Verbreitung von Michelangelo: am 6. März 1992 erlagen nur etwa 10.000 Computer Michelangelos Fluch.

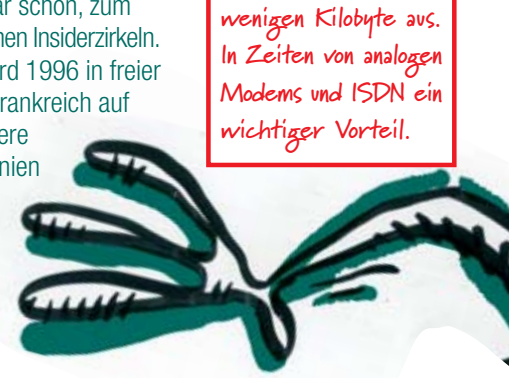
CONCEPT

Papier ist geduldig, virtuelles Papier verwundbar. Mit „Concept“ taucht 1995 der erste Makro-Virus auf. Bis dahin waren Viren in der Regel in Maschinensprache - Assembler – programmiert. Das setzte sehr gute Programmierkenntnisse voraus. Nun nutzten die Autoren zum ersten Mal eine Hochsprache, in diesem Fall WordBasic. Weil Dokumente erheblich häufiger getauscht und verschickt wurden als Dateien, verbreitete sich Concept rasend schnell. Er verfügte über keine Schadroutine, im Virus war folgender Text zu finden: „That's enough to prove my point.” Gerüchten zufolge soll der Autor ein Mitarbeiter von Microsoft gewesen sein. Im Juli 1996 wird der erste Excel-Virus entdeckt – XM.Laroux. AccesiV, der erste Virus für Microsoft Access, folgte im März 1998.

WIN.TENTACLE

Jetzt ist Windows dran. Bislang waren Viren auf DOS, den Boot-Sektor und Makros beschränkt. Viren für Windows gab es zwar schon, zum Beispiel WinVir 1.4, allerdings nur im Labor, in geschlossenen Insiderzirkeln. Mit Win.Tentacle ist auch diese Ära vorbei, der Virus wird 1996 in freier Wildbahn „in-the-wild“ gefunden. Zuerst taucht er in Frankreich auf und legt dort ein Krankenhaus und verschiedenen andere Organisationen lahm. Danach zieht er nach Großbritannien weiter. Er infiziert "exe"-Dateien von Windows, richtet aber in der Regel keinen Schaden an.

Small is beautiful: 1992 führt Kaspersky Lab das Prinzip der Micro-Updates ein. Fortan ist es nicht mehr notwendig, die komplette Antivirus-Datenbank herunterzuladen, eine mittlerweile mehrere Megabyte große Datei. Micro-Updates umfassen nur die Änderungen zwischen der vorhandenen und der neuesten Version der Datenbank und kommen meist mit wenigen Kilobyte aus. In Zeiten von analogen Modems und ISDN ein wichtiger Vorteil.



Nachdem die ersten Linux-Viren aufkommen, ist es höchste Zeit, den Schutz für dieses Betriebssystem zu verstärken. Kaspersky Lab bringt 1999 die erste Sicherheits-Suite für Linux heraus.

LINUX.BLISS

Linux.Bliss wird im Februar 1997 zum ersten Mal beobachtet. Bis dahin war Linux weitgehend von Viren und Würmern verschont geblieben. Die in der Regel strenge Rechtevergabe und die geringere Verbreitung von Linux im Vergleich zu Windows hatten für trügerische Ruhe gesorgt. Mit Linux.Bliss gehört das der Vergangenheit an. Der Virus sucht nach ausführbaren Dateien, die für Schreibzugriffe freigegeben sind und überschreibt sie mit seinem eigenen Programmcode. Danach sucht der Virus nach anderen Hosts, die er infizieren könnte. Netterweise hat der Autor auch gleich ein Gegenmittel eingebaut. Wenn man eine infizierte Datei mit dem Zusatz **„--bliss-disinfect-files-please"** aufruft, löscht sich der Virus selbst.

WIN95.CIH

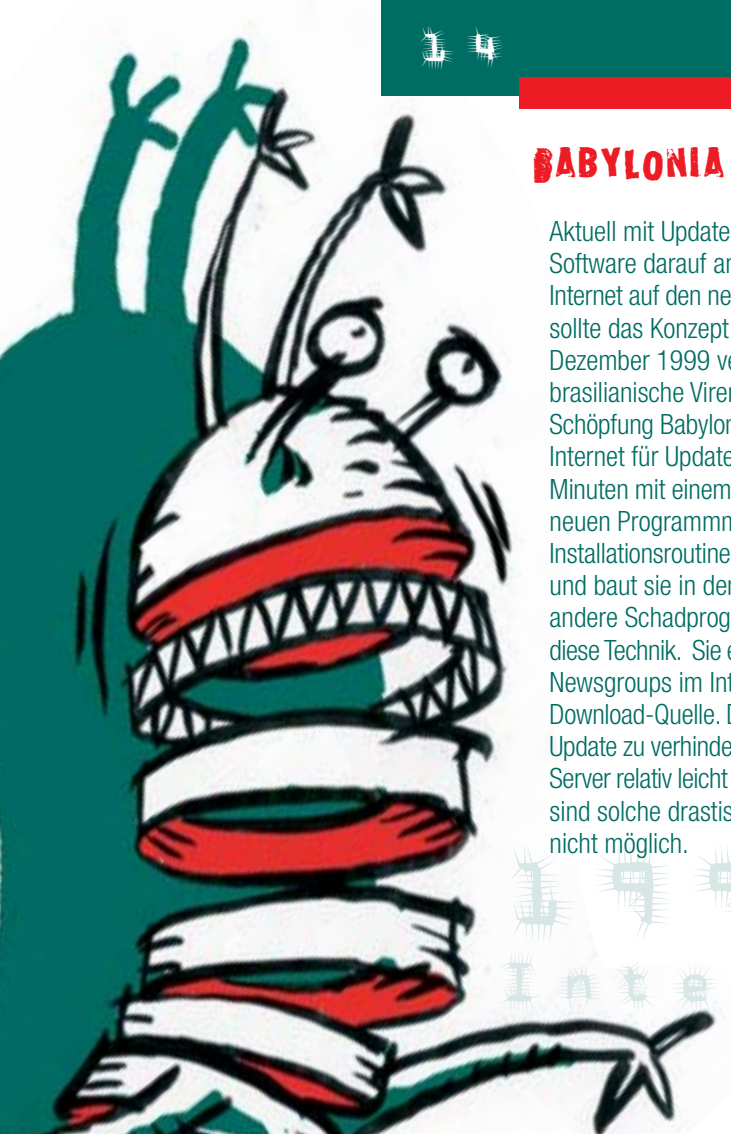
Viren können keine Hardware beschädigen, das galt lange Jahre als unumstößliches Gesetz. Daran zu zweifeln kam dem Glauben an den Weihnachtsmann gleich. Bis Win95.CIH im Juni 1998 auf der Bildfläche erscheint. Der Virus, auch Chernobyl genannt, löscht am 26. April nicht nur Dateien auf der Festplatte, er versucht auch das BIOS der Motherboards zu überschreiben. Gelingt ihm das, ist der Computer ein Fall für den Herstellersupport. Die Schadroutine funktionierte bei einer großen Zahl verschiedener Computertypen, trotzdem hielt sich der Anteil der Betroffenen mit kaputten Motherboards in Grenzen. Win95.CIH verbreitet sich von Taiwan aus rasend schnell. Schon nach einer Woche gelangt der Virus über Raubkopien nach Europa und mausert sich zu einem der meist verbreiteten Schädlinge seiner Zeit. Autor ist der taiwanesische Zivildienstleistende Chen Ing-hau. Er wird verhaftet, aber wieder frei gelassen, weil es keinen Ankläger gibt. Als sein Virus im Jahr darauf wieder aktiv wird, klagt ein taiwanesischer Student, Chen wird zu drei Jahren Haft verurteilt.

MELISSA

Schon in den Achtzigern prophezeien Wissenschaftler, dass E-Mail das ideale Medium für die Verbreitung von Viren ist. Wie recht sie damit hatten, erkennt die Welt am Freitag, dem 26. März 1999. An diesem Tag zeigt „Melissa", wie viel Schaden man mit einer Kombination aus Makro-Virus und Mail-Verbreitung anrichten kann. Sobald der Virus einen PC infiziert hatte, sammelte er 50 E-Mails im Outlook-Adressbuch des Computers und verschickte sich selbstständig an die Empfänger. Der ursprüngliche Benutzer merkte nichts davon, für die Empfänger sah es aber so aus, als würden sie E-Mails von einem Bekannten oder Kollegen erhalten.

Melissa war weder komplex noch besonders boshaft, erreichte aber durch die Anwendung von Social-Engineering-Technik eine enorme Verbreitung. Innerhalb weniger Stunden verteilte er sich in ganz Amerika, dann weiter über die ganze Welt. Als am folgenden Montag Millionen von Beschäftigten ihre PCs einschalten und den Mailclient öffnen, erreicht die Infektionsrate ein exponentielles Maximum. Angeblich werden allein an diesem Tag mehr als 100.000 Computer infiziert. Firmen wie Microsoft, Lockheed Martin und Intel müssen ihre E-Mail-Server komplett abschalten. Das FBI hatte schon am Freitag mit der Suche nach dem Autor begonnen und wird schnell fündig. David L. Smith, Programmierer aus New Jersey und 31 Jahre alt ist für Melissa und damit auch für geschätzte Schäden im zweistelligen Millionenbereich verantwortlich. Er wird im Dezember 1999 zu 10 Jahren Haft und einer Geldstrafe von 400.000 US-Dollar verurteilt.

Im Jahr 1999 entwickelt Kaspersky Lab den ersten Behaviour Blocker für Makro-Viren. Damit hing der Schutz vor bösartiger Software nicht mehr an der Erkennung von Mustern im Virencode ab. Die Behaviour-Analyse schlägt bereits Alarm, wenn Aktionen ausgelöst werden, die nach Virus- oder Wurmaktivität aussehen. Damit schützt diese Technik vor bekannter und unbekannter Schadsoftware.



BABYLONIA | HYBRIS | SONIC

Aktuell mit Updates – heute ist praktisch jede Software darauf angewiesen, sich regelmäßig per Internet auf den neuesten Stand zu bringen. Warum sollte das Konzept vor Viren halt machen? Im Dezember 1999 veröffentlicht der berüchtigte brasilianische Virenautor Vecna seine neueste Schöpfung Babylonia. Der Virus nutzt als erster das Internet für Updates. Er verbindet sich einmal pro Minuten mit einem Server in Japan und sucht nach neuen Programmmodulen. Wird er fündig, lädt die Installationsroutine die aktuelleren Module herunter und baut sie in den Virus ein. Später nutzen auch andere Schadprogramme wie Hybris und Sonic diese Technik. Sie erweitern das Konzept und nutzen Newsgroups im Internet als öffentlich zugängliche Download-Quelle. Dadurch wird es schwieriger, das Update zu verhindern. Während sich anonyme Web-Server relativ leicht blockieren oder schließen lassen, sind solche drastischen Eingriffe bei Newsgroups nicht möglich.

LOVELETTER

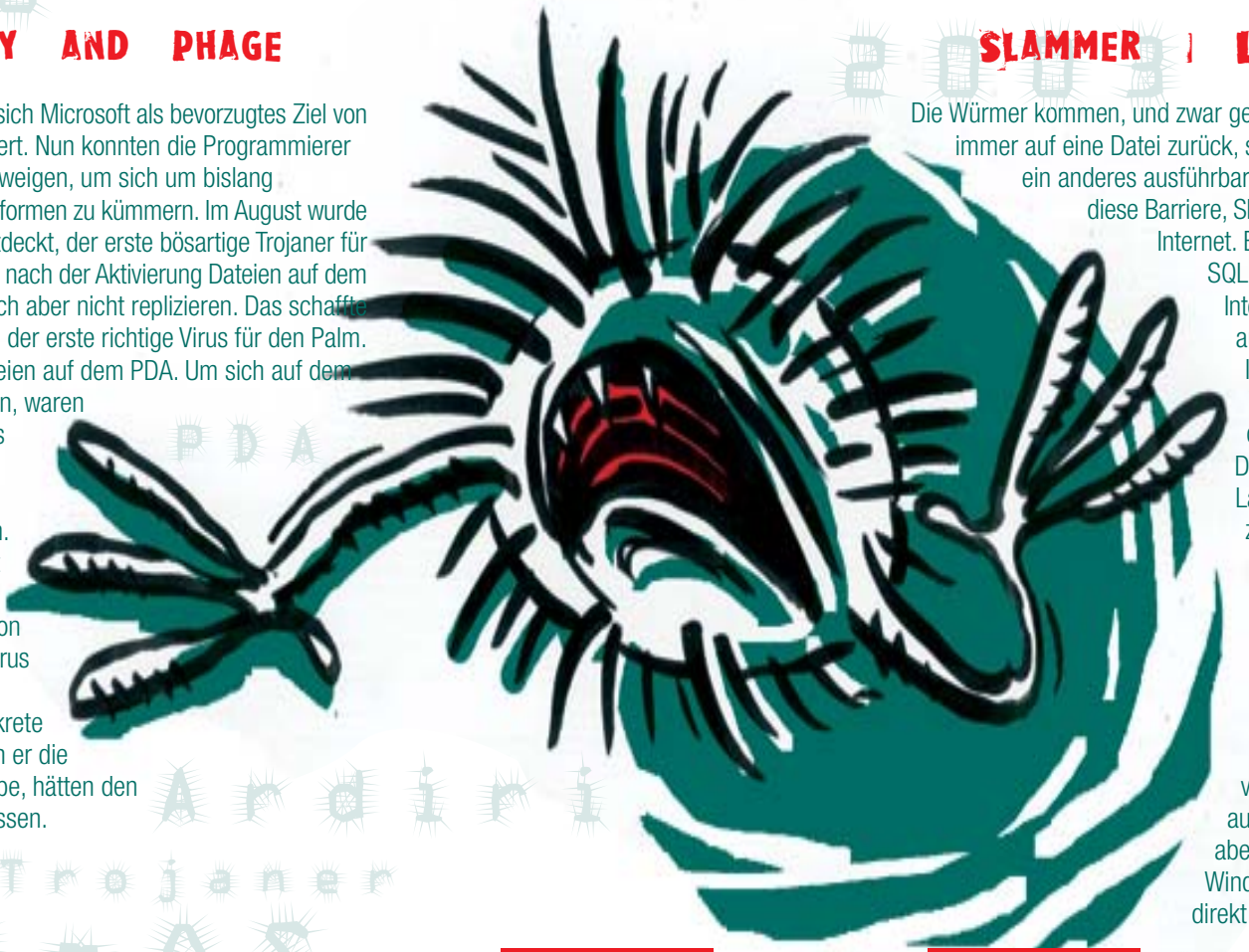
Aufatmen im Jahr 2000. Trotz ernster, manchmal geradezu hysterischer Warnungen, ist die Welt weder untergegangen, noch sind die weltweiten Computernetze zusammen gebrochen. Dafür bedarf es auch keines epochalen Jahrestags, das anscheinend unerschöpfliche Gottvertrauen der Menschen genügt völlig. Anders kann man nicht erklären, was der VBS/LoveLetter- oder auch "iLoveYou"-Virus binnen weniger Stunden anrichtet. LoveLetter verbreitet sich per Mail und enthält einen Anhang im "vbs"-Format. Er wird nicht von sich aus aktiv, sonder muss vom Benutzer angeklickt werden, meist folgt noch eine Bestätigungsabfrage.

Obwohl die Absenderadressen auf den ersten Blick Misstrauen erzeugen sollten, klicken Millionen von Benutzern freudig auf „Ja“ und katapultieren LoveLetter zum erfolgreichsten Virus aller Zeiten. Schon Stunden nach der ersten Entdeckung „in-the-wild“ brechen Mailsysteme aufgrund der hohen Last zusammen. Die verursachten Schäden sollen bereits 2004 mehr als 10 Milliarden US-Dollar betragen haben. Eugene Kaspersky hatte es Jahre vorher bereits angekündigt: „Benutzer sind meist zu naiv, um in einer angehängten Datei bösartige Programme zu vermuten.“ Mittlerweile sind viele Varianten von LoveLetter bekannt und im Umlauf.

Noch 1988 war Peter Norton, bekannt durch seine Tool-Sammlung “Norton Utilities” der Meinung, dass Viren nicht existieren. „Viren sind ein urbaner Mythos,” sagte er in einem Interview mit dem Insight Magazine. „Das ist wie die Geschichte über die Alligatoren in den Abwasserkanälen von New York. Jeder hat davon gehört, aber keiner hat sie jemals gesehen.“ Kurze Zeit später kam die erste Version von Norton Antivirus auf den Markt.

LIBERTY AND PHAGE

Im Jahr 2000 hatte sich Microsoft als bevorzugtes Ziel von Virus-Autoren etabliert. Nun konnten die Programmierer auch etwas Zeit abzweigen, um sich um bislang vernachlässigte Plattformen zu kümmern. Im August wurde der Liberty-Virus entdeckt, der erste bösartige Trojaner für PalmOS. Er zerstörte nach der Aktivierung Dateien auf dem Handheld, konnte sich aber nicht replizieren. Das schaffte etwas später Phage, der erste richtige Virus für den Palm. Auch er löschte Dateien auf dem PDA. Um sich auf dem Handheld einzunisten, waren die beiden allerdings noch auf die Synchronisation mit dem PC angewiesen. Libertys Urherber ist der schwedische Wissenschaftler Aaron Ardiri. Er habe den Virus nur zu Testzwecken programmiert, indiskrete Testpersonen, denen er die Software gezeigt habe, hätten den Virus ins Freie entlassen.



SLAMMER | LOVESAN [BLASTER

Die Würmer kommen, und zwar gewaltig. Bislang gingen Virusinfektionen immer auf eine Datei zurück, sei es nun eine „exe“, „com“, „vbs“ oder ein anderes ausführbares Format. Im Januar 2003 fällt auch diese Barriere, Slammer attackiert aus der Ferne über das Internet. Er nutzt eine Schwachstelle im Microsoft-SQL-Server aus. Alle Computer, die aus dem Internet erreichbar sind und den SQL-Server ausführen, fallen dem Wurm zum Opfer. Innerhalb weniger Minuten infiziert der Wurm Hunderttausende von Computern, die Belastung des Internet steigt auf das Doppelte, komplette Interent-Ländersegmente brechen unter der Last zusammen. Dabei kopiert sich der Wurm nicht einmal auf den befallenen Computer, er bleibt im Arbeitsspeicher und versucht andere Rechner zu infizieren. Wer für Slammer verantwortlich ist, wurde nie geklärt, man geht vom Ursprung im fernen Osten aus. Während Slammer vor allem Firmen betraf – der SQL-Server wird kaum von Privatleuten benutzt – schlug Blaster, auch Lovesan genannt, auch zu Hause zu. Das Prinzip war das gleiche aber Lovesan nutzte eine Sicherheitslücke im RPC-DCOM-Modul von Windows 2000 und Windows XP aus. Dadurch war der Großteil aller direkt mit dem Internet verbundenen PCs betroffen.

Jürgen Kraus verfasst 1980 an der Universität Dortmund eine Diplomarbeit mit dem Titel „Selbst-reproduktion bei Programmen“. Darin stellt er einen Vergleich zwischen Software und biologischen Viren an, und folgert, dass sich Programme wie biologische Viren verhalten könnten. Die Diplomarbeit verschwindet, absichtlich oder nicht, in den Archiven der Universität und wird erst im Dezember 2006 veröffentlicht.

CHOKE

Disketten, E-Mails, die Internet-Verbindung – mittlerweile ist kein Medium mehr vor dem Missbrauch durch Viren sicher. Keines? Doch! Chat-Programme wie der Instant-Messenger erfreuen sich lange Zeit einer unbehelligten Existenz. Bis 2001, dann erscheint Choke auf der Bildfläche. Er verschickt wahllos Nachrichten an ICQ-Benutzer mit dem Text: „Micro$oft invites you to use MSN Messenger!“ Nehmen die angeschriebenen die Einladung an, bekommen sie eine Datei mit Namen wie “ShootPresidentBUSH.exe'” und „choke.exe“ zugeschickt. Ein Doppelklick öffnet dem Virus Tür und Tor.

NETSKY

Musikalisch waren Viren schon früher. In den Achtzigern jodelte der Yankee Doodle die amerikanische Südsstaatenhymne aus infizierten PCs. Eigentlich gilt mittlerweile die Devise: „nur ein unauffälliger Virus ist ein guter Virus“. Doch Netsky bricht mit der Regel. Netsky ist wie Melissa ein E-Mail-Wurm, er versendet sich am 24. März an E-Mail-Adressen, die er in Dateien auf einem befallenen Computer findet. Er enthält sogar seinen eigenen Mailserver, so ist er nicht auf Mailserver im Internet angewiesen, die in der Regel den Massenversand abblocken. Zusätzlich spielen verschiedene NetzSky-Varianten am 2. März zwischen sechs und neun Uhr wahllos Töne aus den PC-Lautsprechern.

BAGLE

Bagle ist ein E-Mail-Wurm wie viele andere. Allerdings führte er das Konzept von Backdoors – Hintertüren – bei PCs ein und erlangte damit traurige Berühmtheit. Er tauchte zuerst im Januar 2004 auf und infizierte PCs mit allen Windows-Betriebssystemen außer dem kaum noch verwendeten Windows 3.11. Nach erfolgreicher Infektion öffnete sich der Windows Taschenrechner oder das Spiel „Hearts“ und Bagle begann, an einem Port auf Nachrichten von Außen zu lauschen. Der Initiator von Bagle erlangte darüber praktisch die volle Kontrolle über den PC und konnte mit ihm nach Gutdünken verfahren. Außerdem versuchte der Wurm Antvirus-Programme abzuschalten oder ihren Start zu verhindern.

Fred Cohen, einer der ersten, der das Potential von Viren erkannte und Gegenmaßnahmen entwickelte, beantragte 1987 Forschungsgelder bei der National Science Foundation. Er wurde mit der Begründung abgewiesen, „dass seine Forschungsarbeit nicht von aktuellem Interesse sei.“

SASSER

Sasser gehört zu den dateilosen Würmern, er infiziert Computer, indem er über das Internet eine bestimmte Sicherheitslücke im Modul LSASS von Windows ausnutzt. Was sich so harmlos liest, führte 2004 zu einer Virenwelle sondergleichen, nur noch übertroffen vom Medienhype, als der Autor Sven J., ein 18-jähriger Schüler aus Norddeutschland, ermittelt wird.

Bald stellte sich heraus, dass er auch für NetSky verantwortlich war. Sasser legte binnen weniger Tage komplette Netzwerke lahm, und verursachte Schäden in Millionenhöhe, und das, obwohl Microsoft bereits lange vor dem Auftreten von Sasser einen Patch für die betreffende Sicherheitslücke im LSASS-Modul bereit gestellt hatte. Sasser veränderte das Sicherheitsbewusstsein in vielen Firmen, automatische Updates wurden danach deutlich häufiger freigegeben und schneller installiert. Trotzdem wimmelt es noch heute im Netz von Sasser-Ablegern.

Sven J. wurde im darauf folgenden Jahr wegen Computersabotage und Datenveränderung zu einer Jugendstrafe von einem Jahr und neun Monaten sowie 30 Stunden gemeinnütziger Arbeit verurteilt.

Ab Juni 2007 sind Denial-of-Service-Attacken in Schweden ein Straftatbestand. Überführte Täter müssen mit Haftstrafen von bis zu zwei Jahren rechnen.

MYDOOM

Keine zentrale Kontrolle, begehrte Inhalte und Hundertausende Benutzer: kein Wunder, dass Tauschnetzwerke wie Kazaa schon seit langem auch als Verteilmedium für Viren heran gezogen wurden. Normalerweise musste man dafür einfach infizierte Dateien zur Verfügung stellen und hoffen, dass der Empfänger keinen aktuellen Virenscanner einsetzt.

MyDoom kann das Tauschnetzwerk Kazaa ganz ohne solche Krücken nutzen. Populär wurde der Wurm allerdings durch seinen primären Daseinszweck – eine Denial-of-Service-Attacke gegen SCO zu starten. SCO war wegen eines Patentstreits eine Weile die meist gehasste Firma im Linux-Umfeld. MyDoom sollte die Website des Linux-Hestellers zwischen dem 1. und dem 12. Februar 2004 angreifen. Allerdings installiert der Wurm auch gleich eine Hintertür im System, über die der Autor vollen Zugriff auf den Computer erhält.

1990 wird in Hamburg das EICAR (European Institute of Anti-Virus Research) gegründet. Heute ist das Institut eine der weltweit am meisten respektierten Einrichtungen im Bereich Computer-sicherheit, praktisch alle namhaften Experten sind Mitglied des EICAR.

Laborvirus

BOS

caribe-sis

Disketten

E-Mail

Internet

Instant Messenger

MP3

Cabir

Symbian-Smartphones

Handy

CABIR

Disketten, E-Mail, Internet, Instant Messenger, was fehlt noch in der Liste der Vireneinfallstore? Richtig, das Handy. Bis Juni 2005 konnte man zumindest beim Telefonieren Vorsichts-maßnahmen vergessen.

Dann wurden die ersten Exemplare von Cabir bekannt, einem Wurm für Symbian-Smartphones, der dessen Bluetooth-Funktion zur Verbreitung nutzt. Zuerst galt er als reiner Laborvirus, der nicht in freier Wildbahn auftauchte. Mittlerweile wurden die ersten Exemplare außerhalb der Entwicklungslabore gefunden.

Sobald ein infiziertes Handy eingeschaltet wird, sucht Cabir nach Bluetooth-Empfängern in seiner Reichweite und verschickt seine Hauptdatei „caribe.sis“ an die erste aktive Verbindung und tarnt sich als Benutzer-oberfläche für ein MP3-Programm. Dennoch geht von Cabir keine große Gefahr aus.
Er fragt mehrfach nach, bevor er sich installiert, das sollte in der Regel eine Infektion verhindern.

GPCode

In den letzten Jahren hat sich eine neue Kategorie von Viren-Autoren gebildet. Es geht nicht mehr ums Prinzip, um die Ehre oder um den Wettbewerb – nun geht es ums Geld, schlicht und einfach.

Deutlichster Vertreter dieser „neuen Schule“ ist GPCode, ein Trojaner, der im Juni 2004 zum ersten Mal auftritt. Nach der Infektion eines Systems verschlüsselt er Dateien. Alles was nach Daten und Informationen aussieht, die dem Anwender lieb und teuer sein könnten, wird mit einem RSA-Algorithmus codiert, die unverschlüsselte Originaldatei gelöscht.

Eine Datei „Readme.txt“ erscheint in den Verzeichnissen, in denen nun verschlüsselte Dateien liegen, sie informiert den Benutzer, dass Daten verschlüsselt wurden und dass man sich für eine Entschlüsselungs-software an eine russische E-Mail-Adresse wenden soll.

Infektion

Cryzip

2004

Ransomware

Nach Untersuchungen im Juli 2005 wurde ein PC mit einem frisch installierten, ungepatchten Windows XP innerhalb von 12 Minuten nach der Verbindung mit dem Internet infiziert.

Schadsoftware die nach diesem Prinzip arbeitet, wird „Ransomware“ (Ransom = Lösegeld) genannt. GPCode und ein naher Verwandter, Cryzip, richten nicht viel Schaden an, auch deshalb, weil der Autor, wie Eugene Kaspersky sagt, „das Crypto-Buch nicht bis zum Ende gelesen hat.“

Eigentlich hätte der Schlüssel von GPCode einen leistungsfähigen PC etwa 30 Jahre beschäftigen sollen. Kaspersky Lab knackte ihn in 10 Minuten. GPCode ist bei weitem nicht der erste Vertreter von Ransomware.

Schon 1989 verschickte Joseph Popp aus Cleveland, Ohio 20.000 mit einem Trojaner infizierte Disketten, der nach und nach alle Verzeichnisse und Dateien auf dem PC verschlüsselte. Ein britisches Gericht erklärte Popp für unzurechnungsfähig, ein italienisches verurteilte ihn zu zwei Jahren Haft in Abwesenheit.

ZOTOB

Sasser hätte eigentlich allen Firmen eine Lehre sein sollen, doch 2005 hatte Zotob nach dem gleichen Muster durchschlagenden Erfolg.

Der Wurm nutzte eine Schwachstelle im Plug-and-Play-System von Windows aus, für die Microsoft bereits einen Patch veröffentlicht hatte. Trotzdem konnte Zotob mehrere große Unternehmen, darunter die Financial Times, CNN, ABC und die New York Times infizieren. Zotob öffnet auf den befallenen Systemen eine Hintertür und suchte aktiv nach weiteren Opfern im Netzwerk.

Der dadurch erzeugte Datenverkehr ließ die Netzwerke zusammenbrechen. Kurz darauf nahmen die marokkanischen Behörden Farid E. und Achraf B. fest und verurteilten sie zu zwei und einem Jahr Haft.

Apples Mac hat einen elitären Status. Was Viren und Würmer angeht, bedeutete das über lange Jahre hinweg völlige Ruhe vor Schädlingen. Doch im Februar 2006 kam auch der Mac im Hier und Heute an.

Der Wurm OSX/Leap-A attackierte Anwender von MacOS X. Er verteilte sich zunächst per Mail und gab vor, im Anhang Screenshots des neuesten Mac Betriebssystem Leopard zu zeigen. Wer die Datei ausführte, fand keine Fotos, wohl aber einen raffinierten Wurm vor, der sich per iChat automatisch an alle Kontakte der Buddylist versendete, sobald diese ihren Status änderten. Weil Leap die Dateiübertragung versteckte, merkten die Betroffenen nichts vom Transfer. Der Wurm enthielt darüber hinaus keine Schadroutine, ließ die Mac-User aber aufhorchen – sie waren nicht mehr immun.

2005

CommWarrior

2004

Cabir

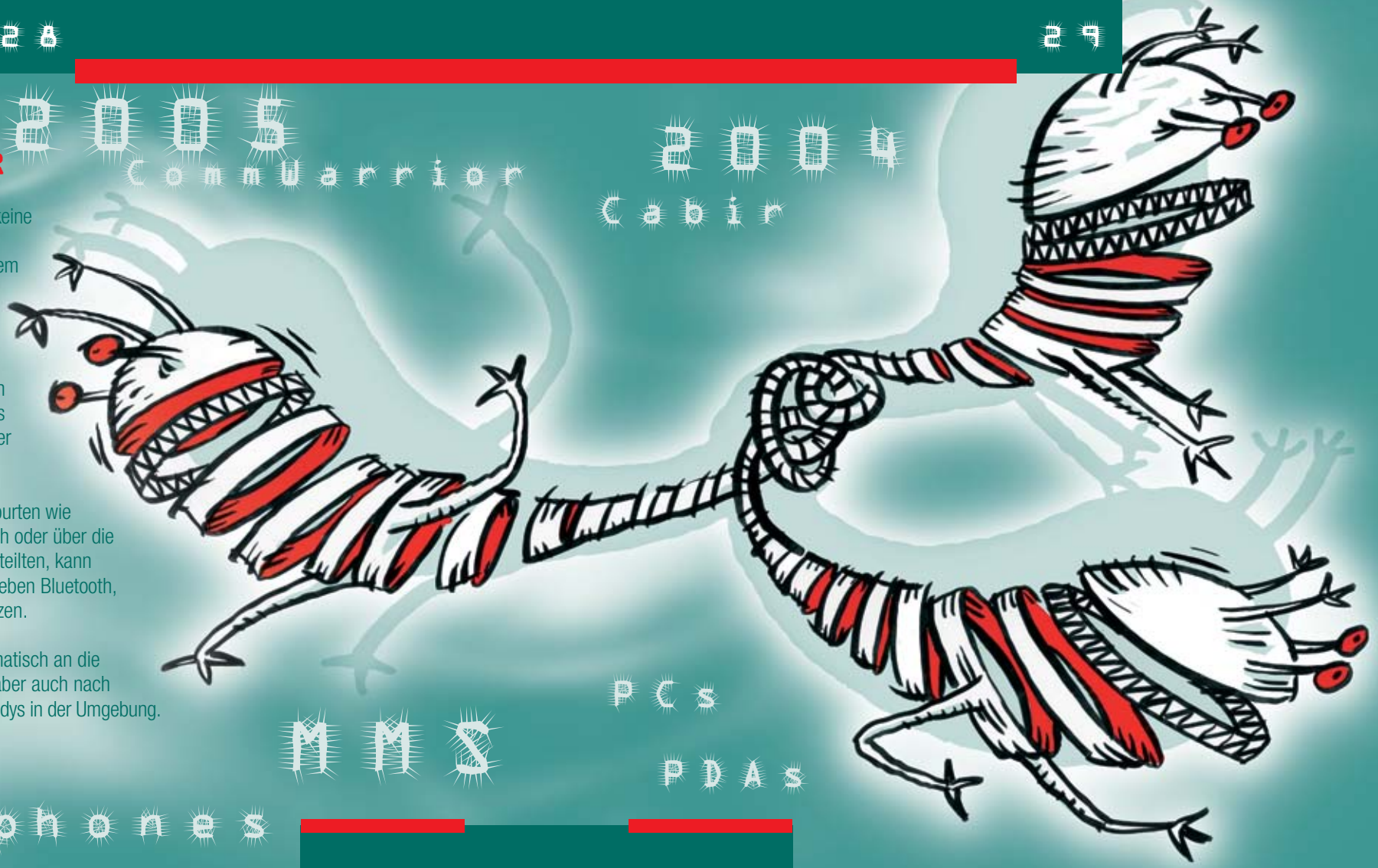
COMMWARRIOR

Schreib mal wieder – aber bitte keine MMS. Denn die könnte mit CommWarrrior verseucht sein, dem ersten Wurm für Multimedia Message Services (MMS).

CommWarrior ist die logische Fortsetzung der Entwicklung. Nach Schadsoftware für PCs und PDAs rückten Smartphones in das Visier der Viren- und Wurmautoren.

Nachdem sich die ersten Ausgeburten wie Cabir im Jahr 2004 per Bluetooth oder über die Synchronisation mit dem PC verteilten, kann CommWarrior ein Jahr später, neben Bluetooth, eine simple MMS als Träger nutzen.

Der Wurm verschickt sich automatisch an die Einträge im Adressbuch, sucht aber auch nach empfangsbereiten Bluetooth-Handys in der Umgebung.



PCs

PDAs

MMS

Smartphones

AdWare

A

Schadsoftware, die sich meist ohne die Einwilligung des Benutzers auf dem PC installiert und Fenster mit Werbung anzeigt oder den Web-Browser zuerst auf nicht gewollte Webseiten umlenkt. In der Regel schwer zu entfernen, oft auch Vehikel, um Trojaner auf einen PC zu bringen.

Backdoor

B

Eine für Benutzer unsichtbare Hintertür im Betriebssystem oder in einem Programm, durch das eine fremde Person Zugriff auf den Computer erlangen kann.

Backdoor-Trojaner

Spezielle Trojaner, die nur die Aufgabe haben, einen PC durch eine Hintertür für fremde Personen freizugeben.

Behaviour Blocker

Als Behaviour Blocker wird ein Programm oder der Teil eines Programms bezeichnet, das in der Lage ist, bestimmte Verhaltensmuster anderer Programme zu erkennen. So lassen sich neue, bislang nicht bekannte Viren und Würmer nur aufgrund ihrer Vorgehensweise, zum Beispiel massenhaftes verschicken von E-Mails, identifizieren und abblocken.

Bootvirus

Die ursprüngliche Form eines Virus. Er infiziert den Bootsektor einer Diskette oder Festplatte. Der Bootsektor gilt als ausführbares Programm, daher wird ein dort versteckter Virus bei jedem Systemstart aktiviert.

Botnet

Ein Zusammenschluss von PCs über das Internet, die in der Regel durch Trojaner infiziert wurden und nun ferngesteuert Aufgaben eines fremden Benutzers ausführen. Botnets werden oft für Denial-of-Service-Angriffe auf Webseiten verwendet oder als unfreiwillige Mailserver zum Versand von Spam-Mail.

Dialer

D

Früher häufig verwendeter Zusatz zu Viren und Würmern. Ein infizierter PC benutze den Dialer um kostenpflichtige Rufnummern anzurufen, die dann über die Telefonrechnung abgerechnet wurden. Mit der hohen Verbreitung von DSL aus der Mode gekommen.

DoS/DDoS-Attacken

(Distributed-)Denial-of-Service-Attacken nutzen meist Botnets um einen Webserver mit so vielen sinnlosen Anfragen zu überschütten, dass keine Kapazitäten für „normale“ Benutzer übrig bleiben. Das Ergebnis ist eine nicht-erreichbare Website und damit Image- und Umsatzverluste beim Opfer.

Exploit

E

Jede Art des Ausnutzens einer Sicherheitslücke für einen Angriff.

Firewall

F

Software oder Hardware, die dazu dient die Verbindungen eines Computers nach Außen und von Außen nach Innen zu kontrollieren. Eine korrekt konfigurierte Firewall ist ein wichtiger Bestandteil des Schutzkonzepts für jeden PC. Firmen nutzen Hardware-Firewalls am Übergang zwischen internem und externem Netzwerk, Privatpersonen sollten zumindest ein Personal Firewall auf Software-Basis nutzen. Die meisten DSL-Router verfügen über eine eingebaute Firewall.

Hacker

In der Computersicherheit ist ein Hacker ein Spezialist, der mit seinem Fachwissen Sicherheitslücken sucht und ausnutzt bzw. dabei hilft, solche Schwachstellen zu erkennen und zu beseitigen. Ein Hacker gilt also als „Guter“, im Gegensatz dazu werden Angreifer als „Cracker“ bezeichnet, allerdings ist diese Begriffstrennung umstritten.

Heuristik

Als Heuristik (griechisch: zu deutsch: ich finde) bezeichnet man Strategien, die das Finden von Lösungen ermöglichen, ohne dass dazu ein festgelegter Weg bekannt ist. Bei Viren wird mit Heuristik eine Methode bezeichnet, um neue, bisher nicht bekannte Schadsoftware zu finden. Mit dieser Technik, ursprünglich entwickelt von Kaspersky Lab, untersucht man den Programmcode einer Datei (oder eines anderen Objekts), um festzustellen, ob darin virusähnliche Befehle enthalten sind. Sobald die Anzahl von virusähnlichen Befehlen ein vorher festgelegtes Maß überschreitet, wird die entsprechende Datei als möglicherweise virusinfiziert markiert. Heuristische Module müssen einen Schwellwert haben, ab dem Alarm gegeben wird.

Hoax

Jede Art von unwahren Virus-, Wurm- oder Trojanermeldungen. Auch Programme die nur als Scherz gedacht sind.

Hybridvirus

Eine Kombination von mehreren Technologien in einem Virus. So wurde beispielsweise der Mobil-Wurm Cabir mit einem Skuller-Virus verschmolzen, das Ergebnis ist ein Hybridvirus.

IM-Wurm

Ein Wurm, der Instant-Messaging wie den Microsoft Messenger als Verbreitungskanal nutzt. Das ist möglich, da IM auch Dateiübertragungen erlaubt.

Intrusion Detection System/Intrusion Prevention System (IDS/IPS)

IDP- und IDS-Systeme überwachen den Netzwerkverkehr auf Protokollbasis und analysieren auf dieser sehr tiefen Detailebene alle Vorgänge. Angriffe auf Netzwerke erfolgen fast immer nach bestimmten Grundmustern, ein gut eingestelltes IDS-System erkennt diese und schlägt Alarm. IDP geht noch weiter: es blockt bei einem festgestellten Einbruchsversuch den Angreifer ab und verhindert dessen Zugriff auf das Netzwerk.

Mobile Viren

Mobile Viren sind Schadprogramme für mobile Geräte wie Smartphones oder PDAs. Sie kamen erst vor verhältnismäßig kurzer Zeit auf, doch ihr Anteil am MMS-Traffic hatte Ende 2006 bereits das Niveau von E-Mail-Schadprogrammen erreicht - 0,5 – 1,5% aller Nachrichten sind infiziert.

Linkvirus

Linkviren hängen sich nicht an eine vorhandene Datei an, sondern manipulieren das Dateisystem. Wird das Zielprogramm gestartet, bleibt der Virus im Arbeitsspeicher und hängt seinen Code an das Programm an.

Nigeria Connection

Umschreibung für eine Form des Online-Betrugs. In einer Mail wird der Empfänger gebeten, gegen eine hohe Provision beim Transport von großen Geldsummen zu helfen. So unwahrscheinlich die Geschichte klingen mag, fallen immer wieder Menschen darauf herein. Im besten Fall verlieren sie diverse Vorschüsse und Gebühren, es kam allerdings schon vor, dass Personen nach Afrika gelockt und dort ausgeraubt und ermordet wurden. Benannt nach dem afrikanischen Land, in dem diese Form des Online-Betrugs einen eigenen Paragraphen im Strafgesetzbuch hat.

Pharming

Beim Pharming fälschen Angreifer, oft mit Hilfe von Trojanern, die Adresse des DNS-Servers für einen PC oder ein ganzes Netzwerk. Anfragen für www.ebay.de landen dann an einem anderen Server, der entweder auf eine gefälschte Seite weiterleitet, oder die Kommunikation mitschneidet um Passwörter zu erbeuten. Der Begriff "Pharming" rührt daher, dass die Betrüger große Server-Farmen unterhalten, auf denen gefälschte Webseiten abgelegt sind.

Phishing

Eine Art des Online-Betrugs, bei dem der Angreifer versucht, den Benutzer zur Preisgabe von Daten wie Passwörtern für das Online-Banking zu bringen. Meist läuft der Angriff über Spam-Mails die zum Besuch einer gefälschten Webseite auffordern.

Polymorpher Virus

Der Begriff „polymorph" leitet sich aus dem Griechischen ab und bedeutet „viele Gestalten". Polymorphe Viren sind variabel verschlüsselt. Sie verstecken sich, indem sie ihre „Gestalt" mit jeder neuen Infektion verändern, damit Virenscanner keine konstante Zeichenfolge für einen vergleich finden.

Proof Of Concept

Funktionsfähige Software, die nur zum Nachweis der Machbarkeit entwickelt wird. Sie tritt in der Regel nicht außerhalb von Forschungslaboren und Entwicklerzirkeln auf.

Ransomware

Schadsoftware, die auf dem infizierten PC reversible Veränderungen vornimmt und diese gegen die Zahlung von Geld wieder rückgängig macht. Bekannt sind Viren, die persönliche Dateien wie Texte oder Tabellen auf dem PC verschlüsseln.

Rootkit

Ein Programm oder eine Sammlung von Programmen, die vor allem die Aufgabe hat, sich der Entdeckung zu entziehen. Ein erfolgreich installiertes Rootkit versteckt sich so gut, dass selbst das Betriebssystem nichts davon merkt. Meist sind auch noch weitere Programme enthalten, die fremden Personen Zugriff auf den Computer gewähren. Rootkits werden schon lange verwendet, erhielten aber vor allem in den letzten zwei Jahren erhöhte Aufmerksamkeit, weil Sony auf einigen CDs einen Kopierschutz mit eingebautem Rootkit verwendete.

Signatur

Der spezifische, unverwechselbare Abdruck eines Schadprogramms. Am Anfang der Antivirus-Entwicklung wurden Viren nur durch einen Signaturvergleich mit einer Datenbank entlarvt, mittlerweile, im Zeitalter polymorpher Viren, kommen auch andere Methoden wie Heuristik und Behaviour Blocker hinzu.

Spam

Jede Art von unverlangt zugesandten E-Mails, Faxen oder Kurznachrichten. Enthalten häufig Viren oder Verweise auf mit Viren verseuchte Websites.

Spyware

Software, die sich unbemerkt vom Benutzer auf dem PC einrichtet und persönliche Daten wie besuchte Webseiten oder auch Passwörter und Benutzernamen aufzeichnet und an fremde Personen weitergibt.

Trojaner (Trojan Dropper, Trojan Downloader…)

Trojaner spiegeln dem Anwender eine andere Funktion vor, als sie tatsächlich haben. So könnte ein Bildschirmschoner mit einem Trojaner versehen sein, der unbemerkt vom Anwender eine Hintertür im Betriebssystem öffnet. Mittlerweile sind Trojan-Dropper beliebt, kleine Programme, die an sich nicht schädlich sind, deshalb auch meist nicht von Antivirus Software erkannt werden und nur die Aufgabe haben, Trojaner aus dem Internet nachzuladen.

Virus

Ein Programm, das ausführbare Programme infiziert, in dem es sich selbst in den ursprünglichen Programmcode hineinkopiert. Kann weitere Funktionen enthalten, ist aber keine Voraussetzung.

Wurm

Benötigt nicht unbedingt ein anderes Programm als Wirt, kann auch als eigenständiges Programm agieren. Wartet im Gegensatz zum Virus nicht passiv auf seine Ausführung sonder versucht proaktiv andere Computer zu infizieren.

Zero-Day-Attacke

Ein Angriff auf eine gerade bekannt gewordene Sicherheitslücke in einem Programm oder Betriebssystem, für die noch kein Patch existiert.

Das kleine Kaspersky-Virenlexikon
erscheint bei der
Kaspersky Labs GmbH
Steinheilstr. 13
D-85053 Ingolstadt
Telefon +49 (0)841 - 981 89 0
info@kaspersky.de

VERTRETUNGSBERECHTIGTER GESCHÄFTSFÜHRER
Andreas Lamm

TEXT
Elmar Török
ProfiNet

REDAKTION
Christian Wirsig, Kaspersky Lab
(V.i.S.d.P. - verantwortlich für den redaktionellen Teil)
Elke Wößner
www.essentialmedia.de

ILLUSTRATIONEN
Florian Mitgutsch
www.mitgutsch.de

LAYOUT
Ahmida Laarab
www.247-design.de

IMPRESSUM

Kaspersky Labs GmbH
Steinheilstr. 13
D-85053 Ingolstadt

Telefon +49 (0)841 - 981 89 0
info@kaspersky.de

www.kaspersky.de
www.viruslist.de