Melissa und ihre Loveletters

Autor(en): **Chien, Eric**

Objekttyp: **Article**

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

Band (Jahr): **80 (2002)**

Heft 7-8

PDF erstellt am: **04.06.2024**

Persistenter Link: https://doi.org/10.5169/seals-877218

Nutzungsbedingungen

Die ETH-Bibliothek ist Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Inhalten der Zeitschriften. Die Rechte liegen in der Regel bei den Herausgebern.
Die auf der Plattform e-periodica veröffentlichten Dokumente stehen für nicht-kommerzielle Zwecke in Lehre und Forschung sowie für die private Nutzung frei zur Verfügung. Einzelne Dateien oder Ausdrucke aus diesem Angebot können zusammen mit diesen Nutzungsbedingungen und den korrekten Herkunftsbezeichnungen weitergegeben werden.
Das Veröffentlichen von Bildern in Print- und Online-Publikationen ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Die systematische Speicherung von Teilen des elektronischen Angebots auf anderen Servern bedarf ebenfalls des schriftlichen Einverständnisses der Rechteinhaber.

Haftungsausschluss

Alle Angaben erfolgen ohne Gewähr für Vollständigkeit oder Richtigkeit. Es wird keine Haftung übernommen für Schäden durch die Verwendung von Informationen aus diesem Online-Angebot oder durch das Fehlen von Informationen. Dies gilt auch für Inhalte Dritter, die über dieses Angebot zugänglich sind.

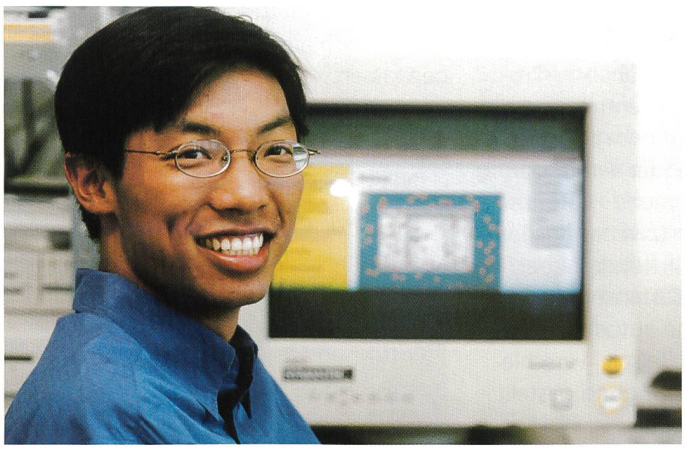
Ein Dienst der *ETH-Bibliothek*
ETH Zürich, Rämistrasse 101, 8092 Zürich, Schweiz, www.library.ethz.ch

http://www.e-periodica.ch

Virenbedrohungen

Melissa und ihre Loveletters

Ein Interview mit Eric Chien, Leiter der Europäischen Zentrale des Symantec Security Response Center (Virenforschungslabor).



Eric Chien, Leiter des Europäischen Virenforschungslabors Symantec Security Response

Herr Chien, sind im Jahre 2001 neue Virentypen aufgetaucht oder waren die Angriffe von Goner und CodeRed lediglich Subvarianten oder Mutationen älterer Viren?

Code Red und Nimda repräsentieren die neuartige Form der gemischten Bedrohung, wenngleich sie technisch betrachtet nicht grundlegend neu sind. Die Viren von heute modernisieren und kombinieren Hackerangriffe und Virencode von gestern. Früher arbeiteten Hacker und Virenentwickler im Allgemeinen getrennt. Virenautoren schrieben schädliche Programme (Malware), die sich vervielfältigen konnten. Hacker hingegen erzeugten Code, der durch Sicherheitslücken wie zum Beispiel Softwarefehler den unbefugten Zugriff auf fremde Systeme ermöglichen sollte.
Durch eine Nachlässigkeit in der Programmlogik des Webservers war es möglich, Programmcode auf dem Zielrechner zur Ausführung zu bringen (Buffer Overflow). CodeRed machte sich diese Art von «Buffer Overflow» zunutze, um auf IIS-Server zu schlüpfen. Nimda benutzte für seine Angriffe eine Eingabebestätigung als Schwachstelle auf IIS-Servern und eine Sicherheitslücke im Mail-Standard MIME (Multi-Purpose Internet Mail Extensions) von Microsoft Outlook.
Durch den vollautomatischen Zugriff brauchen diese Würmer für ihre Verbreitung keine manuelle Hilfe mehr.

Wo liegt der wesentliche Unterschied zu früher und heute?

Früher war die soziale Komponente der Schlüsselfaktor für die Virenausbreitung. Es galt, ahnungslose Anwender zur Ausführung von Viren in Form von E-Mail-Anlagen zu bewegen. Heute ersetzen andere Schwachstellen die Notwendigkeit der sozialen Komponente. Entwickler von Viren können ihre Programme auf dem Zielsystem automatisch ausführen lassen. Somit ist die menschliche Komponente überflüssig geworden.
Die Bedeutungslosigkeit der menschlichen Komponente erhöht die mögliche Ausbreitungsgeschwindigkeit solcher Bedrohungen enorm. In der Vergangenheit hing es sogar vom Wochentag ab, wie schnell sich eine Bedrohung ausbreiten konnte. Der erste erfolgreiche E-Mail-Wurm, W97M.Melissa, wurde beispielsweise an einem Freitag entdeckt, aber erst am folgenden Montag waren die meisten der betroffenen Rechnersysteme wirklich infiziert. Das lag einfach daran, dass die Anwender am Montagmorgen in die Büros kamen, ihre E-Mail lasen und erst damit die Ausbreitung von W97M.Melissa begann.
Im Gegensatz dazu beginnen CodeRed und Nimda sofort mit der Ausbreitung, sobald sie einmal in den Umlauf gelangen. Sie benötigen keine Abfrage von E-Mails, um sich massenhaft auszubreiten. Wie bereits erwähnt, sind diese neuen Viren aber nicht die ersten ihrer Art. Bereits der Morris Internet-Wurm von 1988 infizierte innerhalb von Stunden 10% des Internets, an das zur damaligen Zeit nur rund 6000 Rechner angeschlossen waren. Morris nutzte verschiedene Schwachstellen der damals in Betrieb befindlichen Grossrechnersysteme aus.

Gehören Viren wie zum Beispiel Loveletter der Vergangenheit an?

Es wäre wünschenswert, wenn klassische E-Mail-Würmer wie Loveletter der Vergangenheit angehörten. Doch das ist heute noch nicht der Fall. Viele Anwender arbeiten immer noch nicht nach den Prinzipien des Safe Computing. W32.Goner.A@mm ist ein gutes Beispiel dafür. Es handelt sich dabei um einen einfachen und klassischen Massenmailer für den Versand mit Outlook, der keine speziellen Schwachstellen ausnutzt. Dennoch konnte sich W32.Goner.A@mm schnell und weit ausbreiten, weil die Anwender neugierig auf den vermuteten Bildschirmschoner in der Anlage geklickt haben.

Wie viele Computerschädlinge kennt Symantec Security Response?

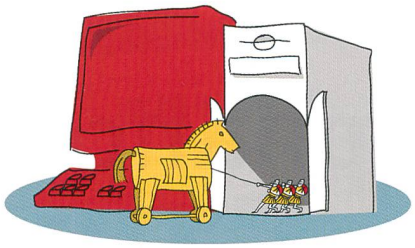
Derzeit sind uns 58 339 Viren, Würmer und bösartige Codes bekannt. Allein im letzten Jahr haben wir mehr als 10 000 neue Viren entdeckt.

Was werden die grössten Virenbedrohungen im Jahr 2002 sein?

2002 werden gemischte Bedrohungen (Hybride) gewiss die Hauptgefahr darstellen. Theoretische Algorithmen sagen voraus, dass es innerhalb von weniger als 20 Minuten möglich sein kann, jeden Rechner im Internet zu infizieren. Das ist noch viel schneller als CodeRed und Nimda sowie Grössenordnungen entfernt von der Ausbreitungsgeschwindigkeit bei VBS.Loveletter und W97M.Melissa.
Anwender müssen ihre Sicherheitsrichtlinien anpassen und dabei auch Updates aller Software-Patches ohne Zeitverzögerung berücksichtigen, besonders wenn diese zum Schliessen von Sicherheitslücken veröffentlicht werden. Bereits einen Monat vor dem Auftreten des arglistigen Codes von Nimda und CodeRed waren Patches verfügbar, die das erfolgreiche Verbreiten verhindert hätten.
Wie bei anderen Technologien sehen wir auch bei den Bedrohungen durch moderne Viren eine Entwicklung, die neben E-Mail auch auf Instant Messaging, Peer-to-Peer-Anwendungen, digitale Geräte und neue Betriebssysteme (Windows XP/.NET) ausgerichtet ist.
Eine Prognose für die Zukunft ist dabei leicht möglich. Aus der Vergangenheit erkennen wir einen klaren Trend: die Malware folgt der technologischen Entwicklung. Vor zehn Jahren waren Grossrechner-Würmer wie der Morris Internet-Wurm von 1988 die Bedrohung. Im Laufe der Jahre entwickelten sich Datei- und Boot-Viren für den PC, weil die Bedeutung der Grossrechner abnahm und dafür jeder einen PC auf dem Schreibtisch stehen hatte. Weil heute immer mehr Leute E-Mail für geschäftliche und private Korrespondenz nutzen, sind E-Mail-Würmer aktuell die grösste Bedrohung geworden.

Können wir im Hinblick auf diese Bedrohungen mit neuen Entwicklungen im Bereich Antivirus-Software rechnen?

Die Evolution der Antivirus-Software geht weg von der reinen Virenschutzlösung. Wir bei Symantec haben unsere Anstrengungen im Bereich der Netzwerk- und Internet-Sicherheit in den letzten zwei Jahren erweitert. Dabei haben wir das Symantec AntiVirus Research Center (SARC) zur Symantec Security Response ausgebaut und weiterentwickelt.



Top Ten Virusliste für 2001 von Symantec Security Response

Europa 2001

1. W95.Hybris.Worm
2. W32.Badtrans.B@mm
3. W32.Sircam.Worm@mm
4. W95.MTX
5. W32.Magistr.39921@mm
6. W32.Magistr.24876@mm
7. WScript.KakWorm
8. W32.Nimda.A@mm
9. W32.CodeRed
10. W32.HLLW.Bymer

Worldwide 2001

1. W95.Hybris.Worm
2. W32.Sircam.Worm@mm
3. W32.Badtrans.B@mm
4. W95.MTX
5. WScript.KakWorm
6. W32.Magistr.39921@mm
7. W32.Magistr.24876@mm
8. W32.Nimda.A@mm
9. W32.CodeRed
10. VBS.Haptime.A@amm

Somit können wir dieselbe Technologie wie für das Update der Virusdefinitionen auch für Updates und Unterstützung in den Bereichen Firewall, Intrusion-Detection-Systeme und Risikomanagement einsetzen. Das alles sind inzwischen wichtige Teile der Rüstung im Kampf gegen bösartigen Codes. Um im Kampf gegen die Entwickler von Viren erfolgreich zu bleiben, können wir uns nicht mehr nur auf die Vervielfältigung von Programmcodes konzentrieren; wir müssen alle Dinge, angefangen von Schwachstellen in Webservern bis zur Funktionsweise von Routern, verstehen.
Seit Viren und Würmer auch Hackermethoden nutzen, sind Intrusion-Detection-Systeme (IDS) der Schlüssel zum Schutz vor neuen Virusinfektionen. In der Zukunft wird der Know-how-Transfer in diesem Bereich eine wichtige Rolle spielen, sodass Antivirus- und IDS-Lösungen auch immer enger zusammenarbeiten müssen.
Weil IDS zur Aufspürung von Hackern ausgelegt sind und Viren sowie Würmer jetzt Hackermethoden einsetzen, werden die Antivirus-Lösungen der Zukunft wahrscheinlich nicht mehr nur Dateien prüfen, sondern auch IDS-Operationen durchführen. Dazu gehören zum Beispiel die Überwachung von Ports und Netzwerkverkehr in Echtzeit sowie von Systemveränderungen in der Registratur oder im Speicher.
Die Situation im Bereich IDS ist heute vergleichbar mit dem Ansehen von Antivirus-Software vor zehn Jahren. Im Vergleich zu Firewalls und zur Virenschutzsoftware nutzen heute nur wenige grosse Unternehmen bereits die IDS-Technologie. In zehn Jahren wird IDS eine standardmässige Sicherheitstechnologie sein, so wie es Firewall und Virenschutz heute sind. Das IDS von morgen wird sich durch eine Verschmelzung von IDS- und Antivirus-Technologien auszeichnen. 4

World Headquarters
Symantec Corporation
20330 Steven Creek Blvd.
Cupertino
CA 95014
USA
Tel. +1 408 517 8000
Hompage: www.symantec.com