Anti-Malware-Systeme: Viren, Würmer und trojanische Pferde

Sebastian Spooren
Timm Kruse

Übersicht der Thematik

1. **Definition von den Begrifflichkeiten**
   1. Malware
   2. Viren
   3. Würmer
   4. Trojanische Pferde
2. **Historie**
   1. Warum alles begann
   2. Wie alles begann
3. **Verbreitungswege**
   1. Verbreitung über E-Mail & Applikationen
   2. Ausnutzung von Sicherheitslücken in Applikationen

Übersicht der Thematik

4. **Identifizierung**
   1. Allgemeines
   2. Spezielle Verfahren
   3. Heuristische Verfahren
   4. Integritätsprüfer
   5. Emulatoren
   6. Einsatz der Verfahren
   7. Geschwindigkeit von Virenscannern
   8. Wie werden neue Viren-Signaturen erstellt?
   9. Die Indizien für ein Virus
   10. F-Prot – Virensignatur vom 23.11.2004

5. **Beseitigung**
   1. Entfernung von Viren
   2. Removal-Tools

Übersicht der Thematik

6. **Lokale und Zentrale Schutzmöglichkeiten vor Malware**
   1. Allgemeines
   2. Zentrale Schutzmöglichkeiten
   3. Lokaler Schutz
   4. Sicherheitsvorkehrungen

7. **Bekannte & aktuelle Meldungen aus dem Malware-Bereich**
   1. Persönliche Erfahrung im IT-Bereich
   2. Details zum Wurm: W32.Blaster
   3. Details zum Wurm: W32.Sober Variante Sober.I

Übersicht der Thematik

8. Zukunftsperspektiven

1. Gegenwart
2. Viren und Spam: Bedrohung in E-Mails
3. Virenbedrohung allgemein
4. Potentielle Bedrohungen durch Mobilität in den Griff bekommen
5. „Code-Check-Tools“ – Das Ende der Sicherheitslücken und Buffer Overflows?
6. Schlusswort

9. Gespräch mit Sophos

1 Definition von den Begrifflichkeiten

1. Malware

- steht für *Malicious Software* und bedeutet schlechte, böswillige Software
- Oberbegriff für schädliche Software wie z.B.: Viren, Würmer, trojanische Pferde

2. Viren

- wird oft synonym mit Malware gleichgesetzt
- nutzen Tarntechniken um sich ungestört zu verbreiten
- keine selbstständigen Programmroutinen
- integrieren ihren Programmcode in Dateien

1 Definition von den Begrifflichkeiten

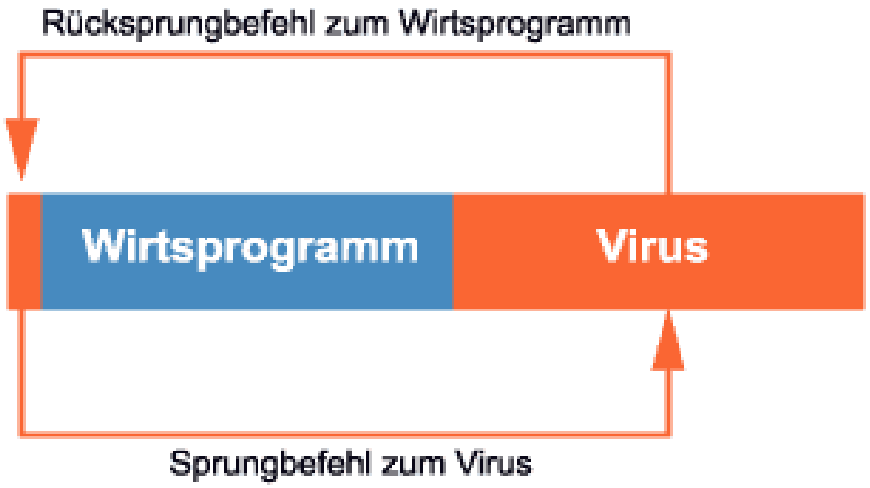
2. Viren

- Schadensfunktion erst nach größerer Verbreitung
- blockieren i.d.R. systemnahe Funktionen
- **Virenarten**
  - Unterscheidung: Viren in freier Wildbahn und Zooviren
  - Bootviren: Befallen Bootsektor, zuverlässige Ausführung
  - Dateiviren: Infizieren ausführbare Dateien
    Replizieren sich beim Aktivieren von Prozessen

1 Definition von den Begrifflichkeiten

2. Viren

- **Virenarten**
  - Dateiviren → anhängendes Virus



  - Polymorphe Viren: verwenden Verschlüsselungsmethoden

1 Definition von den Begrifflichkeiten

2. Viren

- **Virenarten**
  - Stealth-Viren: Benutzen Tarntechniken, um sich vor Anti-Viren-Programmen zu verbergen
  - Makroviren: Schaden i.d.R. auf Dokumentdateien begrenzt

    Erfordern keine besonderen Programmierkenntnisse
  - Multipartite-Viren: Greifen Datei *und* Bootsektor-Records an

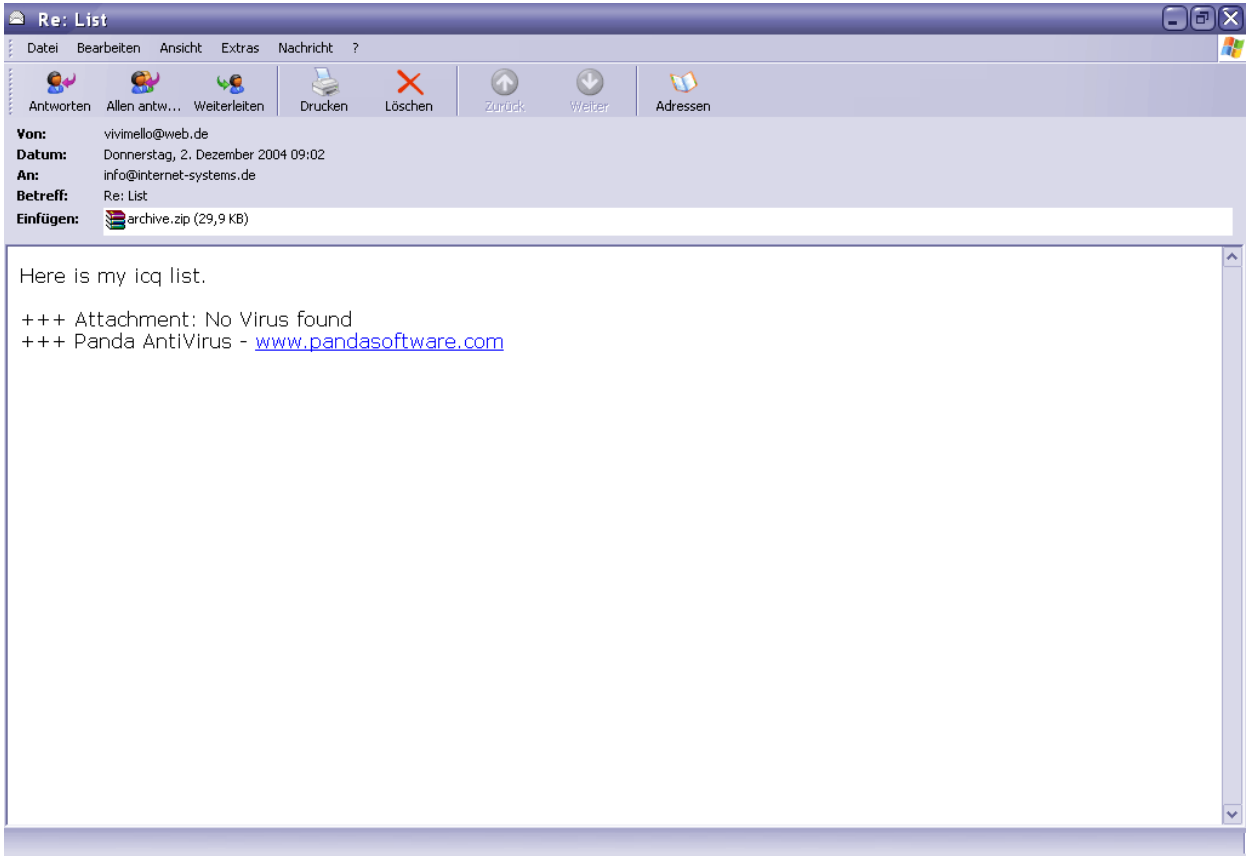
1 Definition von den Begrifflichkeiten

3. Würmer

- benötigen *kein* extra Wirtsprogramm, eigenständige Prozesse
- nutzen Sicherheitslücken in Netzwerken aus oder verschicken sich via E-Mail um sich zu vervielfältigen
- rasante Ausbreitungsgeschwindigkeit
- besonders aggressive Würmer verursachen Schäden in Milliardenhöhe
  - Melissa infizierte innerhalb von drei Tagen 100.000 Rechnersysteme

1 Definition von den Begrifflichkeiten

3. Würmer



1 Definition von den Begrifflichkeiten

4. Trojanische Pferde

- Assoziation mit „Hölzernem Pferd“ aus griechischer Sage Troja
- können Schadroutinen wie Viren und Würmer enthalten
- Backdoor-Trojaner: Client- / Server-Rolle
- Ziel: Ausspähen von Daten (wie Passwörter, vertrauliche Dokumente)

2 Historie

1. Warum alles begann

- Anerkennung in Community
- Spaß, Reiz und Schadenfreude

2. Wie alles begann

- 1982: Entstehung des *ersten* Virus: Elk Cloner

  Programme für verteilte Funktionen mutieren zu *Computerwürmern*

- 1986: erster *PC-Virus*: Brain aus Pakistan

  erster *Dateivirus*: Virdem aus Deutschland

2 Historie

2. Wie alles begann

- 1987: Viren verbreiten sich weltweit an Universitäten
- 1988: erstes *Anti-Virus-Virus* für Brain
- 1989: erster *schnellinfizierender* Virus: Dark Avenger.1800
- 1991: erste *Sicherheitssoftware* von Symantec erhältlich
  - andere folgen

  Veröffentlichung des ersten *Virus-Construction-Sets*
- 1992: weltweit über 2000 Virenarten bekannt

  Mutation-Engine zur Erzeugung polymorpher Viren

2 Historie

2. Wie alles begann

- 1993: Veröffentlichung der ersten *Wild-List*
- 1995: Einführung von Windows 95
  - *Makroviren* entstehen
- 1999: Schnelle Verbreitung von *Melissa* über Massenmails führt zum Absturz vieler Mail-Server
- 2000: *Loveletter* verbreitet sich schneller als Melissa
  - verursacht Schaden in Höhe von $9 Milliarden (Schätzung)
- 2001: *Nimba* manipuliert Web-Server und nutzt nahezu 20 Schwachstellen des Betriebssystems Windows aus

  BadTrans galt bis dato als weit verbreitester Virus weltweit

2 Historie

2. Wie alles begann

- 2002: *BugBear:* erster Wurm mit eigener *SMTP-Engine*
- 2003: *SQL-Slammer* bislang schnellster Wurm

- Auszug aktueller Malware-Meldungen im Detail unter Punkt 7

3 Verbreitungswege

1. Verbreitung über E-Mail & Applikationen

- E-Mail: häufigste Verbreitungsart
- illegale Kopien von Anwendungen und Spielen
- Tauschbörsen
- kleine Software-Applikationen aus unbekannter Quelle
- *Makroviren*: Verbreitung über Dokumente

2. Ausnutzung von Sicherheitslücken in Applikationen

- vermehrte Sicherheitslöcher in Standardsoftware
- ständige Anfragen an offene Ports (Bsp.: Port 445)

3 Verbreitungswege

2. Ausnutzung von Sicherheitslücken *(Screenshot ZoneAlarm)*

Date / Time	Type	Protocol	P	Source IP	Destination IP	Direction
2004/11/24 15:08:42+1:00 GMT	Firewall	TCP (flags:S)		80.143.124.191:4586	192.168.1.1:445	Incoming
2004/11/24 15:08:34+1:00 GMT	Firewall	TCP (flags:S)		80.143.61.52:3910	192.168.1.1:445	Incoming
2004/11/24 15:04:30+1:00 GMT	Firewall	TCP (flags:S)		80.143.170.112:3152	192.168.1.1:445	Incoming
2004/11/24 15:02:02+1:00 GMT	Firewall	TCP (flags:S)		80.143.176.58:4650	192.168.1.1:445	Incoming
2004/11/24 15:01:56+1:00 GMT	Firewall	TCP (flags:S)		80.143.65.186:4217	192.168.1.1:445	Incoming
2004/11/24 15:00:38+1:00 GMT	Firewall	TCP (flags:S)		80.143.189.6:4649	192.168.1.1:445	Incoming
2004/11/24 14:58:26+1:00 GMT	Firewall	TCP (flags:S)		80.143.57.36:1571	192.168.1.1:445	Incoming
2004/11/24 14:58:12+1:00 GMT	Firewall	TCP (flags:S)		80.143.165.36:4827	192.168.1.1:445	Incoming
2004/11/24 14:57:42+1:00 GMT	Firewall	TCP (flags:S)		80.143.228.220:1029	192.168.1.1:445	Incoming
2004/11/24 14:57:24+1:00 GMT	Firewall	TCP (flags:S)		80.143.145.149:1118	192.168.1.1:445	Incoming
2004/11/24 14:57:24+1:00 GMT	Firewall	TCP (flags:S)		80.143.226.241:4265	192.168.1.1:445	Incoming
2004/11/24 14:56:40+1:00 GMT	Firewall	TCP (flags:S)		80.143.61.53:1386	192.168.1.1:445	Incoming
2004/11/24 14:54:50+1:00 GMT	Firewall	TCP (flags:S)		80.143.237.73:4532	192.168.1.1:445	Incoming
2004/11/24 14:54:40+1:00 GMT	Firewall	TCP (flags:S)		80.143.124.240:4033	192.168.1.1:445	Incoming
2004/11/24 14:54:28+1:00 GMT	Firewall	TCP (flags:S)		80.143.170.112:4173	192.168.1.1:445	Incoming
2004/11/24 14:51:40+1:00 GMT	Firewall	TCP (flags:S)		80.143.145.149:1114	192.168.1.1:445	Incoming

3 Verbreitungswege

2. Ausnutzung von Sicherheitslücken

- Exploits: Programme zur Ausnutzung von Sicherheitslücken
- Würmer öffnen *Spammern* Hintertüren
- Virus Cabir: erster *Handy-Virus* nutzt Bluetooth-Schnittstelle aus
- über das Notebook ins Firmennetz

Gefahr ist umso größer, je größer die Netzwerke

Damals: nur bestimmte Regionen betroffen
Heute: weltweite Bedrohung durch das Internet

4 Identifizierung

1. Allgemeines

- erste Anti-Viren-Programme scannen gesamten Dateiinhalt nach bestimmten „Such-String“
- moderne Anti-Viren-Programme arbeiten wesentlich effizienter durch Beschränkung auf Dateibereiche
- Skriptviren bleiben vorerst unentdeckt, da sie erst bei Ausführung sichtbar werden
- immer bedeutsamer wird das Entdecken von *polymorphen Viren*

4 Identifizierung

2. Spezielle Verfahren

- Suche nach bestimmtem „Such-String“ (engl. „Search-String“)
- Nachteil: jede kleine Veränderung macht das Verfahren untauglich
  Es werden nur bekannte Viren erkannt

3. Heuristische Verfahren

- Entwicklung neuer Methoden, um unbekannte Viren zu entdecken
- Einsatz von allgemeinem „Such-String“, bei nur kleineren Varianten, führt zur Erkennung des Schädlings
- Dateizugriffsüberprüfung nach festgelegten Regeln
  Bsp.: Zugriff auf Bootsektor, Adressbuch

4 Identifizierung

3. Heuristische Verfahren

- falls Risiko als „hoch“ bewertet, Anzeichen für Virenbefall
- Trojaner erschweren das Auffinden, da sie sich wie „normale“ Programme verhalten: keine Verbreitungsroutinen

4. Integritätsprüfer

- Validierung anhand der Prüfsumme

5. Emulatoren

- geschützte Umgebung zur Entfaltung der Viren

4 Identifizierung

6. Einsatz der Verfahren

- perfekte Kombination aller Methoden
- Test der Virenscanner mit alter Virensignaturliste, jedoch neues Virus

7. Geschwindigkeit von Virenscannern

- sortierte Virendatenbank
- Beschränkung der Suche auf wesentliche Teile
- etwa die Hälfte der Zeit beansprucht den Zugriff auf Dateien
- Wächterprogramme bremsen das System

4 Identifizierung

8. Wie werden neue Viren-Signaturen erstellt?

- Einsendungen von verdächtigen Programmen an das Anti-Viren-Labor
- Monitoring-Tools überwachen jeglichen Zugriff auf Speicher
- Durchführung von Tests zur Ermittlung eines „Such-Strings“
- bei „normalen“ Viren i.d.R. etwa 40 Minuten für Analyse, Signatur und Removal-Tools
- bei komplexen Viren muss ein Spezialist die Arbeit übernehmen es kann mehrere Tage dauern
- jeden Tag erscheinen mehrere Versionen neuer Viren-Definitionslisten

4 Identifizierung

9. Die Indizien für ein Virus

- Absturz nach Ausführung eines sonst stabilen Programms
- häufige Festplattenaktivität, obwohl kein Programm aktiv ist (Voraussetzung: Scheduler deaktiviert)
- seltsame Bildschirmmeldungen (Fehlermeldungen)

4 Identifizierung

10. F-Prot – Virensignatur vom 23.11.2004

Malware-Typ	Anzahl
DOS/Windows	59.975
Unix/Linux	409
Makro (Office)	8.283
Java	245
PalmOS	4
Script (VB, JavaScript, Unix Shell, IRC, INF)	7.657
Batch und andere (AMi, PIF, PHP, WinBAT, BAT)	2.957
zerstörende Programme	55.405
insgesamt Viren, Würmer, Trojaner und Backdoors	134.935

5 Beseitigung

1. Entfernung der Viren

- standardisierte Vorgehensweise:
  Virenscanner löschen schädlichen Code aus Datei
- keine 100%ige Sicherheit auf unversehrte Daten,
  falls das Virus Daten überschrieben hat
- eventuelle Entfernung von Einträgen aus der Registry

2. Removal-Tools

- ist die genaue Wurmbezeichnung bekannt:
  Einsatz von individuellen Removal-Tools
- des Weiteren existieren allgemeine Removal-Tools zur
  Entfernung der am weitest verbreiteten Würmer

5 Beseitigung

Virus im Firmennetz (IBM)

6 Lokale und Zentrale Schutzmöglichkeiten vor Malware

1. Allgemeines

- Technik alleine liefert keinen 100%igen Schutz
  - der Benutzer stellt ein großes Gefahrenpotential dar

2. Zentrale Schutzmöglichkeiten

- größter Verbreitungsweg über E-Mail
  → Ansatz beim Mailserver: *Mailwall*

  Vorteil: Sie filtern Viren schon beim Versand aus
  Nachteil: Führt zu hoher Serverauslastung

- Virenscanner und Firewalls sollten insbesondere an Endpunkten vor oder auf Netzkoppelelementen zum Einsatz kommen

  Vorteil: Komplettes Netzwerk geschützt

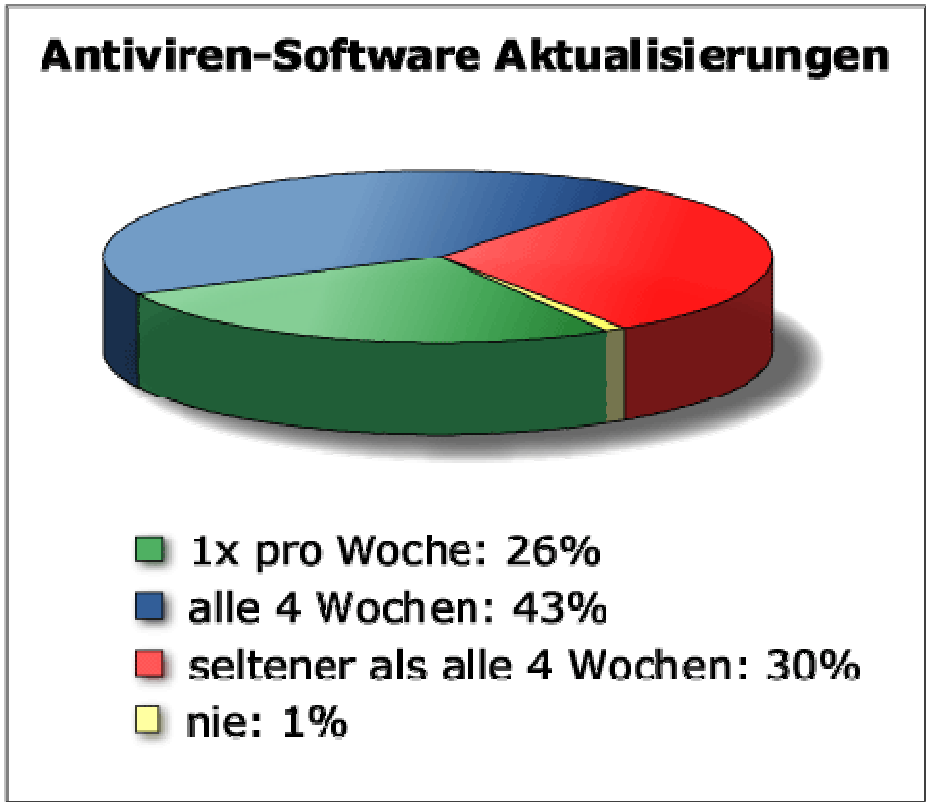
6 Lokale und Zentrale Schutzmöglichkeiten vor Malware

2. Zentrale Schutzmöglichkeiten

- Netzwerk-Überwachungstool mit dem der Administrator via Fernzugriff alle Sicherheitsanwendungen kontrollieren und updaten kann

6 Lokale und Zentrale Schutzmöglichkeiten vor Malware

3. Lokaler Schutz



6 Lokale und Zentrale Schutzmöglichkeiten vor Malware

4. Sicherheitsvorkehrungen

- Öffnen von Dateianhängen nur unter Vorsicht
- Virenwarnungen via E-Mail (meistens *Hoaxes)* mit Vorsicht interpretieren
- Einsatz eines sicheren Browsers
- neuste Updates installieren (z.B. Service Pack 2)
- aktuelles Anti-Viren-Programm und Firewall einsetzen

6 Lokale und Zentrale Schutzmöglichkeiten vor Malware

4. Sicherheitsvorkehrungen

- Live Update aktivieren, bzw. selber täglich neue Viren-Signaturen laden
- regelmäßige Backups
- aktuelle Sicherheitsmeldungen einholen
- sichere Kennwörter verwenden und häufig ändern
- Vorsicht bei Benutzung von Tauschbörsen und kleinen Applikationen aus dem Internet

7 Bekannte & aktuelle Meldungen aus dem Malware-Bereich

1. Persönliche Erfahrung im IT-Bereich

- Unternehmen entspricht mitunter höchster Qualitäts- und Sicherheitsnorm (vergl. mit anderen Unternehmen der Branche)
- erste Anzeichen für Virenbefall:
  - Mehrere Rechner starteten unaufgefordert neu
  - VoiceOverIP-Telefonanlage äußerst eingeschränkt nutzbar
- Folge: Technische Kommunikation völlig außer Betrieb
- Ursache: Befall des Wurmes W32.Blaster

7 Bekannte & aktuelle Meldungen aus dem Malware-Bereich

2. Details zum Wurm: W32.Blaster

- verbreitet sich weltweit, aufgrund einer Sicherheitslücke in MS-Windows, rasend schnell
- entdeckt am 11.08.2003
- Sicherheitslücke: Fehler in DCOM RPC (Remote-Process-Control)
- direkt betroffen: MS-Windows NT Systeme
  zusätzliche Betriebssysteme, die RPC Schnittstelle installiert haben
- Ziel: Microsoft auf unsichere Software hinweisen
  16.08.2003 DoS-Attacke gegen Windows-Update-Server
- auch andere Betriebssysteme betroffen
- http://www.pandasoftware.com/virus_info/flash/mapa_popup.asp?idioma=2&color=F1F8FC

7 Bekannte & aktuelle Meldungen aus dem Malware-Bereich

3. Details zum Wurm: W32.Sober Variante Sober.I

- verbreitet sich via E-Mail
- entdeckt am 19.11.2004
- Aliase: WORM_SOBER.I, W32.Sober.I@mm, W32/Sober.I, Sober.J
- Absender: unterschiedlich
  Betreff: unterschiedlich (täuscht Fehler beim Mailprovider vor)
  Nachricht: unterschiedlich (unterscheidet zwischen englischen und deutschen E-Mail-Adressen)
- Größe des Dateianhangs: 56.808 Bytes, 46.056 Bytes
- Dateiname: unterschiedlich
- Dateiendung: unterschiedlich, kann aus *doppelten* Endungen bestehen, z.B. name.txt.com

7 Bekannte & aktuelle Meldungen aus dem Malware-Bereich

3. Details zum Wurm: W32.Sober Variante Sober.I

- betroffen: Windows 2000, Windows 95, Windows 98, Windows Me, Windows NT, Windows Server 2003, Windows XP
- in Microsoft Visual Basic geschriebene Variante von Sober.H
- mit Laufzeitpacker UPX gepackt
- erstellt in Windowsverzeichnissen Dateien mit zufälligen Namen
- durchsucht Dateien (.php, .htm, .ppt und viele weitere) nach weiteren E-Mail-Adressen und verschickt sich an diese weiter
- versendet E-Mails über eigens mitgeführte SMTP-Engine
- überprüft Verbindung zum Internet mit NTP-, DNS-Anfragen
- es wird ein rechtsradikaler Hintergrund vermutet, so wie es auch bei Sober.H der Fall war

7 Bekannte & aktuelle Meldungen aus dem Malware-Bereich

3. Details zum Wurm: W32.Sober Variante Sober.I

Ergebnisse von AV-Test:

Wann wurde die neue Sober Variante von den jeweiligen Virenscannern erkannt?

Produkt	Uhrzeit	Erkannt als
AntiVir	07:48	Worm/Sober.I
Panda	08:26	W32/Sober.I.worm
Bitdefender	08:50	Worm32.Sober.I@mm
Avast	09:16	Win32:Sober-H
AVG	09:28	I-Worm/Sober.I
Kaspersky	09:46	I-Worm.Sober.i
Trend Micro	10:09	WORM_SOBER.I
F-Secure	10:16	I-Worm.Sober.i
Sophos	10:35	W32/Sober-I
Dr. Web	10:55	Win32.HLLM.Sober
McAfee	12:09	W32/Sober.j@MM
Symantec	12:41	W32.Sober.I@mm
RAV	16:40	Win32/Sober.I@mm

8 Zukunftsperspektiven

1. Gegenwart

- PC´s, die sich ohne Sicherheitssoftware im Internet befinden, sind innerhalb von 20 Minuten infiziert
- jeder war schon mal betroffen und viele wissen meist gar nicht, dass ihr Rechner infiziert ist
- homogene Softwarelandschaft ermöglicht bessere Verbreitung der Malware
- Kommunikationsdichte enorm gewachsen (234 Mio. Hosts)

2. Viren und Spam: Bedrohung in E-Mails

- E-Mail als wichtigste Unternehmensanwendung gerät durch E-Mail Attacken außer Kontrolle:
  Wichtige E-Mails lassen sich nicht problemlos filtern

8 Zukunftsperspektiven

3. Virenbedrohung allgemein

- 70% der europäischen Unternehmen befürchten in den nächsten zehn Jahren eine Verdopplung der Virenangriffen
- das Verhältnis zwischen Viren und E-Mails lag 2002 bei 1:212 und heute bei 1:10

4. Potentielle Bedrohungen durch Mobilität in den Griff bekommen

- ändernde Sicherheitseinstellungen nach Umgebung (z.B. Arbeitsplatz und Heimnetz)
- moderne Sicherheitssysteme beziehen Updates automatisch
- Self-Defending Network von Cisco ermöglicht Einstufung der Benutzer in unterschiedliche Sicherheitszonen

8 Zukunftsperspektiven

5. „Code-Check-Tools“ – Das Ende der Sicherheitslücken und Buffer Overflows?

- Vorbeugung bei der Erzeugung von SourceCode vor Sicherheitsrisiken
- Microsoft bietet Schulungen über sichere Speicherverwaltung (Eindämmung von Buffer Overflows)
- Einsatz der Tools ermöglicht Ausmerzung von relevanten Sicherheitslücken auf breiter Ebene
  → Wunschgedanke: Zukünftig qualitativ gute Software entwickeln

8 Zukunftsperspektiven

6. Schlusswort

- Microsoft setzt Belohnung zur Aufdeckung von Virenautoren aus ($250.000)
- Zitat vom Pressesprecher Alex Günsche der Protect Privacy Organisation:

  „Die Wahrheit liegt, wie so oft, irgendwo in der Mitte. Ein Ende der Viren-, Würmer- und Spam-Seuche ist genau so illusorisch wie der ewige Weltfrieden.“

- keine Änderung vorausschaubar, im Gegenteil zunehmende Malware
- Einsatz von Virenscanner und Firewall schon heute unabdingbar
- Einsatz von Schutzmöglichkeiten auf zentraler Ebene nach Möglichkeit in Echtzeit

9 Gespräch mit Sophos

- **Fragen an Sophos**
  - Wie viele Viren (gesamte Malware) werden derzeit mit Ihrem Programm erkannt?
  - Wie lange dauert heutzutage das Verfahren zur Erzeugung einer Anti-Viren-Routine bzw. die Erstellung eines Removal-Tools?
  - Wie gut sind Heuristik-Verfahren?
  - Wie viele Viren-, Würmer-, Trojaner-Neuerscheinungen haben Sie in etwa pro Tag?
  - Was war ihr größter Anti-Viren Erfolg?

10 Literatur und Quellenangabe

Bücher:

Dr. Karlhorst Klotz – Dr. Klotz' Computerschutz
Verlag: mitp

Das Anti-Viren-Buch – David Harley, Robert Slade, Urs E. Gattiker
Verlag: mitp

anonymous – hacker's guide – Sicherheit im Internet und im lokalen Netz
Verlag: Markt & Technik

Online-Referenzen:

http://www.bul-online.de
http://www.antivirus-online.de
http://www.kreideholen.de
http://www.emsisoft.de/de
http://www.heise.de
http://www.antivir.de
http://www.trendmicro.com
http://www.virus-informer.de
http://www.virusbtn.com
http://www.theparallax.org
http://www.poose.de
http://www.trojaner-info.de
http://www.golem.de
http://online.securityfocus.com
http://www.symantec.de
http://www.bsi.bund.de
http://www.virus-aktuell.de
http://www.cisco.com