Viren, Würmer und Trojaner

Verbundstudium TBW
Veranstaltung IKS

Jochen Voigt und Hans Faber

Inhaltsfolie

- Viren
  - Definition / Prinzip
  - Grundtypen
  - Schaeden / Vorbeugende Massnahmen
- Trojaner
  - Definition / Prinzip
  - Grundtypen
  - Schaeden / Vorbeugende Massnahmen
- Wuermer
  - Definition / Prinzip
  - Grundtypen
  - Schaeden / Vorbeugende Massnahmen

Viren

- Definition:

  Nicht selbststaendige Programmroutine, die sich selbst reproduziert und nicht kontrollierbare Manipulationen in Systembereichen oder an anderen Programmen vornimmt

- Prinzip:

  Jeder Virus benoetigt ein Wirtsprogramm, an das er sich lagert oder das er ueberschreibt. Somit wird zuerst der Virus-Code und dann das urspruengliche Programm ausgefuehrt.

Viren

Grundtypen von Viren:

1. Boot-Virus: Befindet sich im Boot-Sektor einer Diskette oder Festplatte und wird durch einen Kalt- oder Warmstart des PC aktiviert
2. File-Virus: Ist in einem Wirtsprogramm enthalten und wird durch Aufruf dieses Programms aktiviert
3. Makro-Virus: Nistet sich in Steuersequenzen von Daten-Dateien ein. Laeuft beim Arbeiten mit Daten-Dateien automatisch ab, z.B. MS Excel.
4. Skript-Virus: Ausfuehrung eines Programms durch einen Interpreter. Fuegt sich nach Infektion in den Skriptbereich z.B. einer HTML Datei ein. Wird nach dem Laden ausgefuehrt.

Viren

Schaeden:

- personell
- öffentliche / nationale Sicherheit
- immateriell / Ansehen
- Rechtsverstöße
- finanziell und
- materiell

Viren

Vorbeugende Massnahmen:

- Regelmaessig Datensicherung durchfuehren
- Aktuelle Viren-Schutzsoftware verwenden
- Ein- und ausgehende Datentraeger und Programme aus Mails / Internet auf Viren pruefen
- Mitarbeiter ueber Viren schulen
- Effiziente Rechteverwaltung, nicht ohne Grund als Administrator angemeldet sein

Trojaner

- Definition:

  Programme, die neben scheinbar nuetzlichen auch schaedliche Funktionen enthalten und diese ohne Wissen des Anwenders eigenstaendig ausfuehren. Im Gegensatz zu Viren verbreiten sie sich nicht selbstaendig.

Trojaner

Grundtypen von Trojanern:

1. Linker: Heftet ein zweites, “schlechtes” Programm an eine beliebige Wirtsdatei sodass beide Programme gestartet werden
2. Dropper: Startet heimlich eine Installationsroutine eines “schlechten” Programms. Automatischer Programmstart nach jedem Neustart eines PCs
3. Plugin: “Schlechter” Erweiterungsbaustein fuer ein Programm, Hinzufuegen weiterer Funktionen, z.B Browser-Plugin

Trojaner

Grundtypen von Trojanern:

4. Schnittstelle: Oeffnet mit Hilfe eines Internet Browsers ein verstecktes Fenster und baut eine Verbindung mit dem Internet auf. Tastatureingaben und Passwoerter werden so an den Angreifer geschickt. Firewalls sind wirkungslos, da Verbindungen zum Internet fuer den Browser erlaubt wurden.

Trojaner

Schaeden:

- Ueberwachung des Datenverkehrs oder aller Benutzeraktivitaeten durch Sniffer
- Ausspaehen und Weiterleiten von Passwoertern, Kreditkartennummern oder Kontonummern
- Installation von illegalen Dialer-Programmen zur heimlichen Einwahl auf eine teure Telefon-Mehrwertnummer
- Als Speicherressource zur Ablage von illegalen Dateien

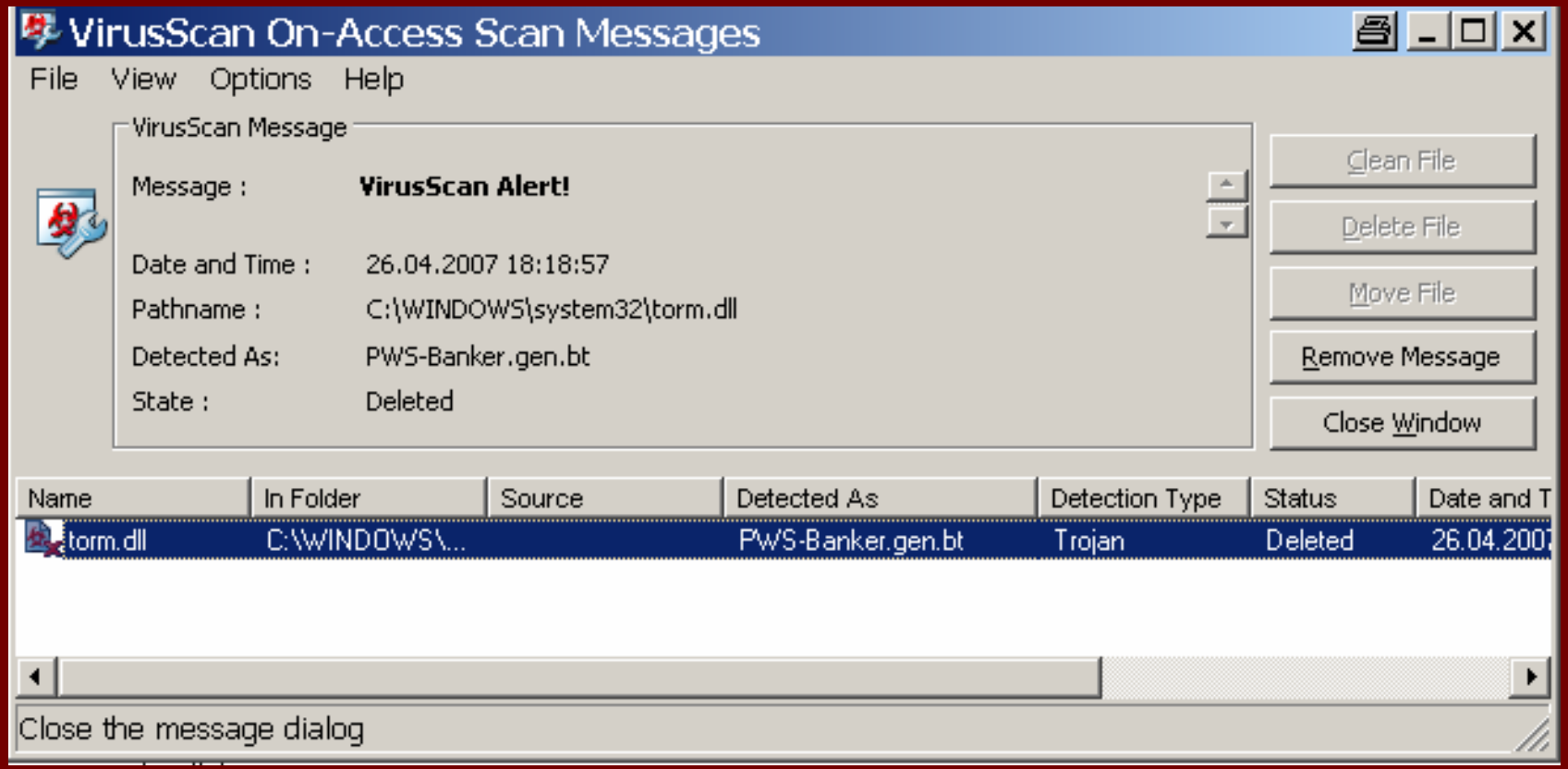
Trojaner

Vorbeugende Massnahmen:

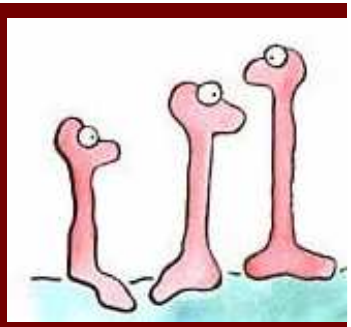
- Verzicht auf die Benutzung von Programmen aus unbekannten oder unsicheren Quellen
- Aktuelle Viren-Schutzsoftware verwenden. Manche Trojaner deaktivieren Antivirenprogramme oder manipulieren das System, sodass sie nicht mehr erkannt werden
- Personal Firewalls zur Netzwerkueberwachung
- Bestrebungen der Trusted Computing Group, das Ausfuehren ungepruefter Software technisch unterbindbar zu machen

Trojaner

Beispiel fuer einen erfolgreich abgewehrten Angriff eines Trojaners durch McAfee VirusScan



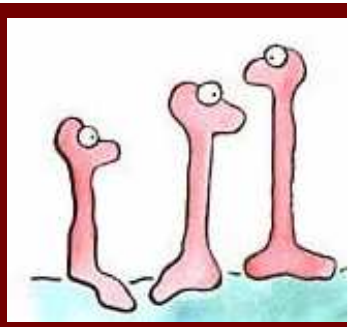
Wuermer



- Definition: Verbreiten sich im Gegensatz zu Viren aktiv via Email oder Netzwerk. Heute haeufig Mischformen wie Trojanerwuermer

- Prinzip am Bsp. Email: Wurm verschickt eine Kopie von sich als Emailanhang. Ziel, dass der Empfaenger diesen oeffnet. Tarnung des Anhangs durch doppelte Dateinamens-erweiterung (z.B. faber.ppt.exe), wenig bekannte Dateinamensendungen (z.B. faber.vbs), als ZIP-Datei

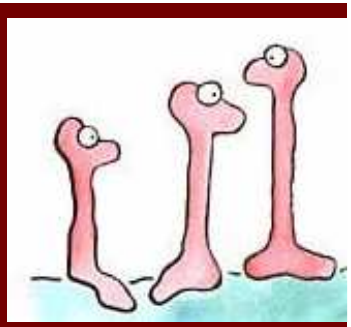
Wuermer



Grundtypen von Wuermern:

1. Instant Messaging Wuermer, z.B. ICQ: Link zu einer verseuchten Seite wird allen Kontakten automatisch geschickt. Wurm wird bei Anklicken des Links installiert, ausgefuehrt und verbreitet sich weiter
2. IRC-Wuermer: Infektion durch Einloggen und Schreiben von Meldungen in einem Internet Relay Chat durch Modifikation des Start-Skriptes

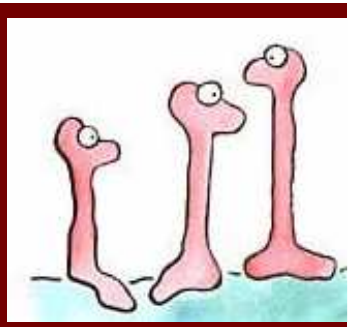
Wuermer



Grundtypen von Wuermern:

3. Peer-to-Peer Wuermer: Verbreitung ueber Tauschboersen wie Kazaa
4. Handywuermer: Verbreitung ueber Bluetooth, MMS oder Bordcomputer von Autos durch Angriff auf das Betriebssystem Symbian OS

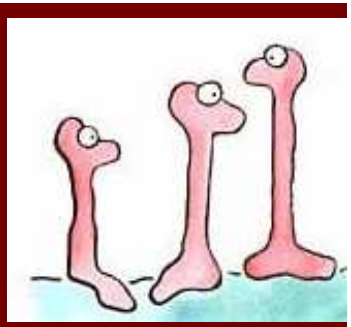
Wuermer



Schaeden:

- Um vieles hoeher als bei Viren durch enormen Verbrauch an Netzwerkressourcen mit ggf. dessen Ausfall. Z.B. Anzeigetafel am Flughafen Wien-Schwechat 2004 durch Wurm Sasser oder lahmgelegte Server der estlaendischen Regierung durch Distributed-Denial-of-Service-Attacke durch Wurm W32.Blaster
- Seit 2003 Kopfgeld auf Wurmautoren ausgesetzt, Initiator Microsoft
- Prominente Wuermer: Netsky, Sobig, I love you

Wuermer



Vorbeugende Massnahmen:

- Sorgfaeltige Pruefung von Emailanhaengen
- Virenscanner
- Personal-Firewalls
- Paketfilter: Netzwerkkommunikation wird durch individuelle Konfiguration gefiltert
- Rechtetrennung des Betriebssystems: Weitestgehender Verzicht von Arbeiten mit Administratorrechten unter Windows, da viele Sicherheitsschranken ausser Kraft gesetzt

Viren, Würmer und Trojaner

Quellen:

www.bsi.de

www.wikipedia.de

www.heise.de

Bundesamt für Sicherheit in der Informationstechnik

heise online

Jochen Voigt und Hans Faber