

# Malware

# Inhalt

- 1 Viren und Würmer
- 2 Trojaner
- 3 Malware Protection

# Viren

## Geschichtliches:

- 1949 Idee, dass ein Computerprogramm sich selbst wieder herstellen kann
- 1950 Idee in Spiel umgesetzt
- 1982 wurde erster Bootsektorvirus programmiert
- 1985-1990 wurden MS-DOS, Apple Macintosh, Amiga, Atari und Unix Opfer von ersten Virenangriffen ⇒ Ersten Antivirenprogramme entwickelt
- 1990-1995 DOS-Viren
- 1995-2002 32-Bit-Windows Viren
- ab 2002 Anfang der Würmer

# Viren

## Was sind Viren:

- Verbreiten sich, indem es sich in noch nicht infizierte Dateien kopiert und diese dann ausgeführt werden.
- Diese Kopien haben folgenden Ziele:
  - 1 Ausführen von Schadcode
  - 2 Weiteres Eindringen in andere Ressourcen des Computers

# Viren

## Datei-Viren:

- Am häufigsten anzutreffende Virentyp
- Virus muss sich in diese Wirtsdatei einfügen (oft am Ende)
- Wirtsdatei wird so modifiziert, dass das Virus beim Programmstart aufgerufen wird
- Eindringen auf unterschiedliche Art und Weise in ausführbaren Dateien

## Bootsektor-Viren:

- Sind die ältesten Viren
- Bootsektoren von Disketten bzw. Festplatten werden infiziert
- Bootsektor wird bei jeden Start des Betriebssystems ausgeführt
- Heutzutage aber so gut wie Ausgestorben

# Viren

## Marko-Viren:

- Sind nicht eigenständige Programme, sondern in Form von Makros
- Makros sind Programme, die in Dokumenten eingebettet sind
- Darunter fallen: Microsoft Word, Microsoft Excel, Microsoft PowerPoint ...
- Meistens Ziel, die Standardvorlage zu infizieren da diese bei jedem Programmstart automatisch geladen wird und der Virus so automatisch mit aktiv wird

## Berühmte Viren:

- Das Jerusalem-Virus:  
führte erstmals zu bleibenden Schäden. Löscht am Fr. 13. alle .exe und .com Dateien
- Das Michelangelo-Virus:  
Bootsektor Virus. Wurde am Geburtstag von Michelangelo aktiv
- Das Concept-Virus:  
Gilt als der erste Makro-Virus. Entstand durch Tatsache, dass mehr Dokumente als Programme ausgetauscht wurden



## Geschichtliches:

- 1997 verbreitet sich der erste E-Mail-Wurm Namens ShareFun
- 1999 verbreitet sich Über E-Mail der Wurm Melissa weltweit
- 2001 erscheinen erste Würmer mit einer eigenen SMTP-Engine
- 2005 erscheint mit SymbOS.Commwarrior der erste Wurm, der sich selbst als MMS verschicken kann

## Was sind Würmer?

- Im Gegensatz zu Viren dringen Würmer aktiv auf neue Systeme ein
- Nutzen Sicherheitslücken des Betriebssystems aus wie Netzwerkdienste oder Anwendungen die Netzwerkdienste beanspruchen
- Ein Wurm kann sich wie ein Virus in andere Programmdateien einnisten

## E-Mail-Würmer:

- Benutzen zur Verbreitung E-Mail Dienste
- Versenden E-Mail mit einer Datei oder einem Link als Anhang
- Durchsucht E-Mail Kontaktliste und versendet sich selbständig weiter

## IM- und IRC-Würmer:

- Benutzen zur Verbreitung Whatsapp, ICQ, MSN Messenger oder IRC-Clients
- Ähnlich wie bei E-Mail-Würmer versendet dieser einen Link an andere Kontakte mit der Schadhaften Datei
- Durchsucht Kontaktliste und versendet sich selbständig weiter

## Berühmte Würmer:

- Melissa:  
Versendet Mails an Kontakte und führt zu Überlastung
- Der Sasser-Wurm:  
Verbreitete sich nicht per Mail, sondern nutzte Schwachstelle von Windows-Dienst LSASS. Schaltet Computer in unregelmäßigen Abständen aus
- ILOVEYOU:  
Verbreitete sich extrem schnell mit einem Anhang namens LOVELETTER. Löscht div. Dateien und ersetzt diese mit .vbs Dateien

# Trojaner

- 1 Geschichte
- 2 Was sind Trojaner
- 3 Verbreitung
- 4 Was ist ihr Ziel
- 5 Bundestrojaner

# Geschichte

- Name stammt vom Sieg der Griechen im Kampf gegen Troja
- Hölzernes Pferd mit Griechen darin
- Krieg gewonnen, weil sie unbemerkt in Troja waren



# Was sind Trojaner?

- Programme, die gezielt in Computer eingeschleust werden
- als nützliches Programm oder Software getarnt
- kann wirklich nützliche Funktionen enthalten
- Virus schon im Programm oder erst aus Internet heruntergeladen
- keine Weiterverbreitung im Gegensatz zu Viren und Würmern



# Was sind Trojaner?

- keine selbstständige Reproduktion
- Schadprogramm läuft eigenständig auf PC
- Start der Schadsoftware
  - 1 mit PC
  - 2 mit bestimmten Programm
- löschen und beenden funktioniert nicht

# Verbreitung von Trojaner

- mittels E-Mail (Anhang)
- P2P Websites und diverse Websites
- Werbe-CDs
- USB

# Aktivitäten der Schädlinge

Es werden meist unbemerkt Aktionen durchgeführt, wie zb Daten sammeln, welche im Internet übermittelt werden.

- Spionage
- Daten Diebstahl
- bis zur Zerstörung vom System

# Arten von Trojanern

## ■ Sniffer

- 1 aufzeichnen, auswerten, übertragen
- 2 Keylogger
- 3 Passwortspionage

## ■ Backdoor

- 1 Kontrolle wird übergeben
- 2 Hacker kann alle Aktionen ausführen
- 3 Zusammenschluss krimineller Zwecke

## ■ Dropper

- 1 installiert andere Schadsoftware
- 2 versteckt Schädlingsprogramme

## ■ Linker

- 1 verbindet schädliche Trojaner oder Programme
- 2 nicht sichtbar auf PC

## ■ Exploit

- 1 nutzt Fehlerfunktionen und Sicherheitslücken
- 2 Manipulation von Computeraktivitäten (Administrationsrechte)
- 3 Internetserver lahm legen

## ■ Rootkit

- 1 Angreifer installieren verschiedene Schadprogramme
- 2 dauerhafter Zugriff auf Computer
- 3 schwer auffindbar mit Antivirus-Software
- 4 fungieren als Backdoors

## ■ Trojan Banker

## ■ Werbe- Trojaner

# Erkennung von Trojanern

## Windows:

- beenden, herunterfahren
- Taskleiste verbirgt sich
- seltsame Meldungen in Dialogfenster
- Systemfarben ändern sich
- Laufwerke öffnen und schließen sich

## OSX und Linux:

- Malware ist nicht so stark verbreitet

# Bundestrojaner

- Online Durchsuchung
- staatliche Spähsoftware zur Strafverfolgung
- Kommunikationsnetzwerke werden durchsucht vom Staat
- kann mehr als nur Telekommunikation aufzuzeichnen
- gesamte Daten auf Gerät erlangen oder manipulieren

# Bundestrojaner Deutschland

- 1 Rechtsgrundlage nochmals verändert nach Terroranschlägen
- 2 2009 - Wohnungen überwacht
- 3 Telefonate belauscht
- 4 Reformiertes BKA Gesetz - Grundlage für Bundestrojaner
- 5 jahrelanger Rechtsstreit - Bestandteile BKA verfassungswidrig
- 6 Schutz von Privatsphäre nicht gesichert
- 7 Beweise von Spionage können vor Gericht verwendet werden
- 8 nur Daten aus laufenden Telekommunikationen



# Bundestrojaner Österreich

- 1 2007 Schadsoftware von DigiTask erworben
- 2 diskussion über Zulassung in Österreich
- 3 gegen Terror und Mordvergehen
- 4 Whatsapp und Skype
- 5 noch keine Gesetzes Grundlage
- 6 Einsatz der Software nicht geplant

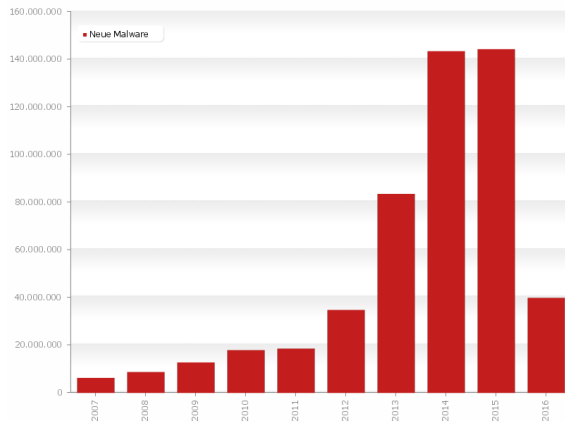


# Malware Scanning

## Themen:

- 1 Malware Statistik
- 2 Erkennungsrate vs. Infektionswahrscheinlichkeit
- 3 Performance-Efficiency-Tradeoff
- 4 Malware Scanning
  - Static Scanning
  - Dynamic Scanning
  - Heuristic/Proactive Scanning

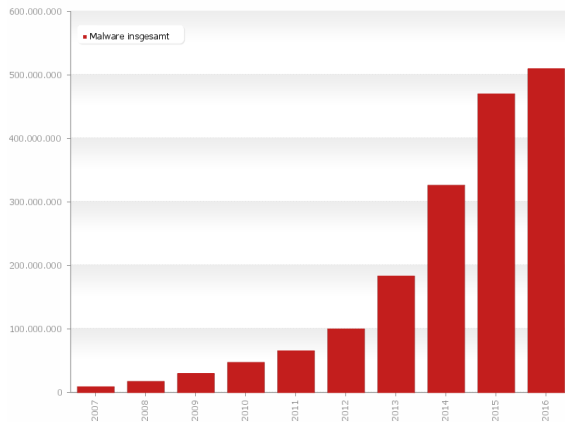
## Neue Malware



Letzte Aktualisierung: 06.04.2016 14:15

Copyright © AV-TEST GmbH, [www.av-test.org](http://www.av-test.org)

## Gesamte Malware



Letzte Aktualisierung: 06.04.2016 14:15

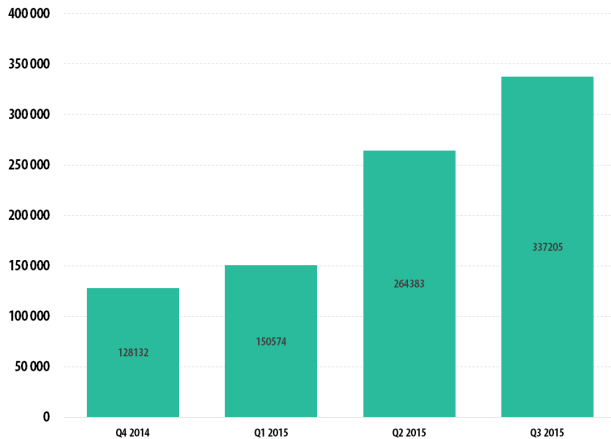
Copyright © AV-TEST GmbH, [www.av-test.org](http://www.av-test.org)

# Ransomware

## Definition

Wichtige persönliche Daten auf dem Computer der Opfers werden verschlüsselt und sind daher nicht mehr verwendbar. Den Entschlüsselungs-Key erhält man erst nach der Überweisung eines Lösegelds (ransom).

## Ransomware



© 2015 AO Kaspersky Lab. Alle Rechte vorbehalten.

## Hauptkriterien:

- Erkennungsrate vs. Infektionswahrscheinlichkeit
- Performance-Effectivity-Tradeoff
- Scanning Techniken

# Erkennungsrate vs. Infektionswahrscheinlichkeit

Infektionswahrscheinlichkeit  $\neq 1 - \text{Erkennungsrate}$

Infektionswahrscheinlichkeit bei  $n$  voneinander unabhängigen Angriffen:

$$p_{\text{Befall}} = (r_x)^n$$



# Performance-Effectivity-Tradeoff

Hohe Effektivität → hoher Leistungsverbrauch → niedrige Performance

Hohe Performance → niedriger Leistungsverbrauch → niedrige Effektivität

Kompromiss zwischen Performance und Effektivität

# Static Scanning

## Static Scanning

- 1 Codeausschnitt aus Datei
- 2 Vergleich mit Codeausschnitten in Datenbank
- 3 Entscheidung, ob Virus oder nicht

# Static Scanning

## Vorteile

- Erkennt Malware mit festgelegter Signatur garantiert
- Datei muss nicht geöffnet/ausgeführt werden

## Nachteile

- Übersieht unbekannte Schädlinge
- Erkennt keine alternativen Versionen
- Erkennt nur exakte Treffer
- Speicherverbrauch für Datenbank

# Dynamic Scanning

## Dynamic Scanning

- 1 Verhalten in Verhaltenskatalog gespeichert
- 2 Überprüft Verhalten bei Öffnen/Ausführen
- 3 Vergleicht Verhalten mit Katalog
- 4 Blockiert Programm oder lässt Ausführung zu

# Dynamic Scanning

## Vorteile

- Unbekannte Malware kann erkannt werden

## Nachteile

- Schwierig alle Verhaltensweisen festzuhalten
- Kann evtl. Verhalten nicht erkennen
- Kann keine völlig neuen Schädlinge erkennen
- False-Positives: Blockiert gutartige Programme

# Heuristic/Proaktive Scanning

## Heuristic/Proaktive Scanning

- Bestimmt Wahrscheinlichkeit schädlichen Verhaltens
- Führt Datei nicht aus
- Blockiert Programm aufgrund berechneter Wahrscheinlichkeit
- Meist über Sandbox realisiert

# Scanner umgehen

Malware kann nur gefunden werden wenn:

- Signatur in der Datenbank existiert
- Verhalten in der Datenbank existiert
- Heuristische Untersuchung eine hohe Wahrscheinlichkeit für schädliches Verhalten ermitteln

# Scanner umgehen

Malware kann nur gefunden werden wenn:

- Signatur in der Datenbank existiert
- Verhalten in der Datenbank existiert
- Heuristische Untersuchung eine hohe Wahrscheinlichkeit für schädliches Verhalten ermitteln

Design neuer Malware:

- Neue Signatur oder komplett neues Verhalten kann von keinem Scanner erkannt werden
- Gefahr besteht, bis Änderungen in Anti-Malware integriert
- Integration von Signaturen schnell, von Verhaltensregeln langsam
- Bis zur Aktualisierung: kein Schutz



# Schlussfolgerung

Ein guter Scanner muss:

- alle Scanning-Techniken Kombinieren
- dadurch eine sehr hohe Erkennungsrate haben
- einen Kompromiss zwischen Performance und Effektivität finden
- Regelmäßig mit Updates versorgt werden

# Schlussfolgerung

Trotz der Erfüllung dieser Voraussetzungen sitzen Malware Entwickler immer am längeren Ast. Wird eine komplett neuartige Malware entwickelt, muss diese erst identifiziert, sowie Regeln und Signaturen dafür erstellt werden. Bis zu dem Zeitpunkt, zu dem das Update an User ausgeliefert wird, sind deren Geräte der neuen Malware schutzlos ausgeliefert

**Vielen Dank für eure  
Aufmerksamkeit**