Malware

Inhalt

1 Viren und Würmer
2 Trojaner
3 Malware Protection
4 Anwendungsbeispiel

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 $\Rightarrow$ Entwicklung erster Antivirenprogramme
- 1990-1995 DOS-Viren
- 1995-2002 32-Bit-Windows Viren
- ab 2002 Computerwürmer

Viren

Was sind Viren:

- Verbreiten sich, indem sie sich in noch nicht infizierte Dateien kopieren, die 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 die Wirt-Datei einfügen (oft am Ende)
- Wirt-Datei wird so modifiziert, dass das Virus beim Programmstart aufgerufen wird
- Dringen unterschiedliche Art und Weise in ausführbaren Dateien ein

Viren

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 keine eigenständigen Programme
- treten in Form von Makros auf
- Makros sind Programme, die in Dokumenten eingebettet sind
- Darunter fallen: Microsoft Word, Microsoft Excel, Microsoft PowerPoint ...
- Ziel: Standardvorlage infizieren da diese bei jedem Programmstart automatisch geladen wird $\rightarrow$ Virus automatisch mit aktiviert

Viren

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. Überschreibt ersten 100 Sektoren der Festplatte mit Nullen
- Das Concept-Virus:
  Gilt als der erste Makro-Virus. Editiert das NORMAL.DOT template von Microsoft Word. Er erzeugt eine Dialog Box mit Nummer 1 und einem OK Button

Würmer

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

Würmer

Was sind Würmer?

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

Würmer

E-Mail-Würmer:

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

Würmer

IM- und IRC-Würmer:

- Benutzen zur Verbreitung Whatsapp, ICQ, MSN Messenger oder IRC-Clients
- Ähnlich wie bei E-Mail-Würmer versenden diese einen Link mit der schadhaften Datei an andere Kontakte
- Durchsuchen Kontaktliste und versenden sich selbständig

Würmer

Berühmte Würmer:

- Melissa:
  Versendet Mails an Kontakte und führt zu Überlastung
- Der Sasser-Wurm:
  Verbreitete sich nicht per Mail, sonder nutzte Schwachstelle vom Windows-Dienst LSASS. Schaltet Computer in unregelmäßigen Abständen aus
- ILOVEYOU:
  Verbreitete sich extrem schnell mit einem Anhang namens LOVELETTER. Löscht div. Datein 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 eindringen konnten

Was sind Trojaner?

- Programme, die gezielt in Computer eingeschleust werden
- als nützliche Programme oder Software getarnt
- können tatsächlich nützliche Funktionen enthalten
- Virus ist schon im Programm oder wird erst aus Internet heruntergeladen
- Im Gegensatz zu Viren und Würmern keine Weiterverbreitung

Was sind Trojaner?

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

Verbreitung von Trojaner

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

Aktivitäten der Schädlinge

Es werden meist unbemerkt Aktionen durchgeführt, z.B. Daten gesammelt, welche via Internet übermittelt werden.

- Spionage
- Daten Diebstahl
- bis hin zur Zerstörung des Systems

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 für kriminelle 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. lahm legen von Webservern
- Rootkit
  1. Angreifer installieren verschiedene Schadprogramme
  2. dauerhafter Zugriff auf Computer
  3. mit Antiviren-Software schwer auffindbar
  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 vom Staat durchsucht
- 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 verfassungswidrig
6. Schutz von Privatsphäre nicht gesichert
7. Beweise aus Spionageaktionen können vor Gericht verwendet werden
8. nur Daten aus laufender Telekommunikation

Bundestrojaner Österreich

1. 2007 Schadsoftware von DigiTask erworben
2. Diskussion über Zulassung in Österreich
3. Anwendung gegen Terror und Mordvergehen
4. Whatsapp und Skype
5. noch keine Gesetzesgrundlage
6. Einsatz der Software nicht geplant

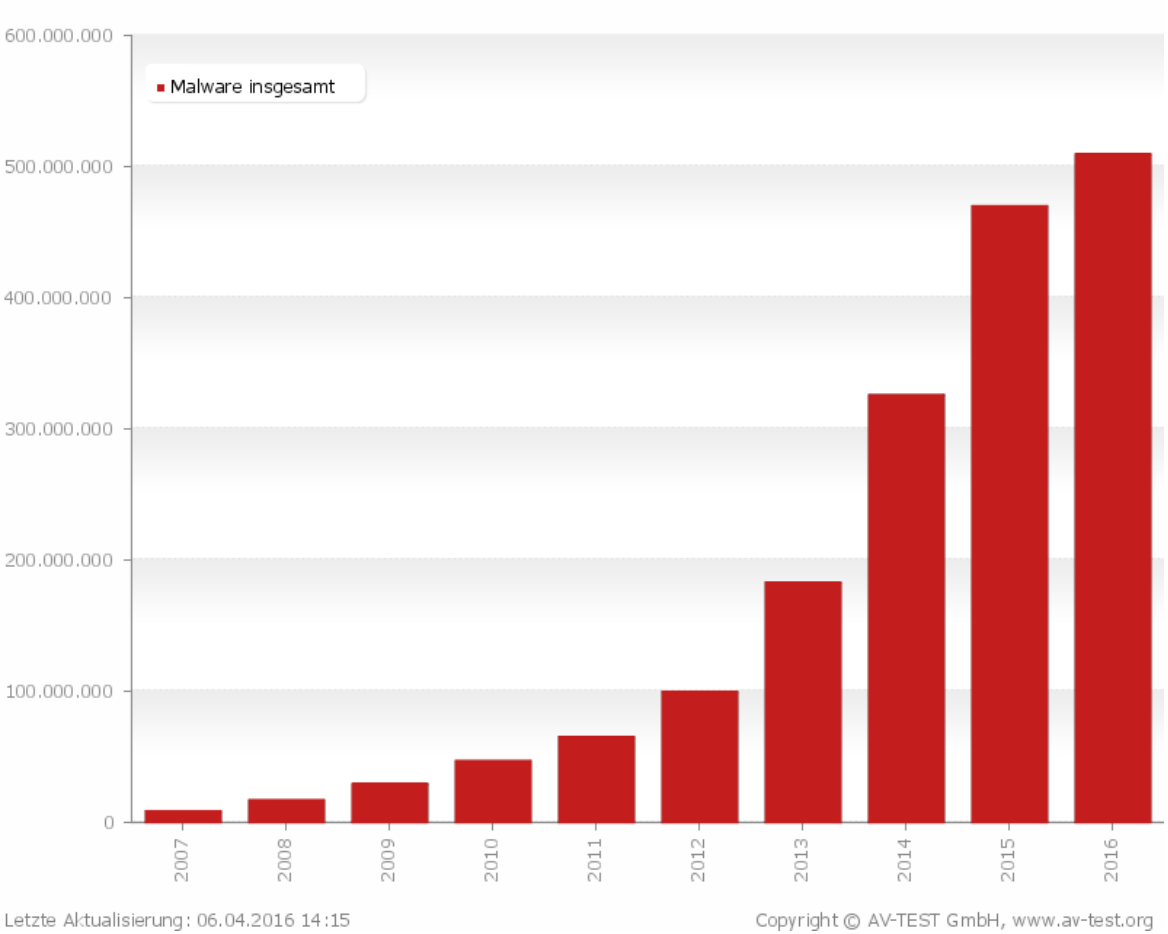
Malware Scanning

Themen:

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

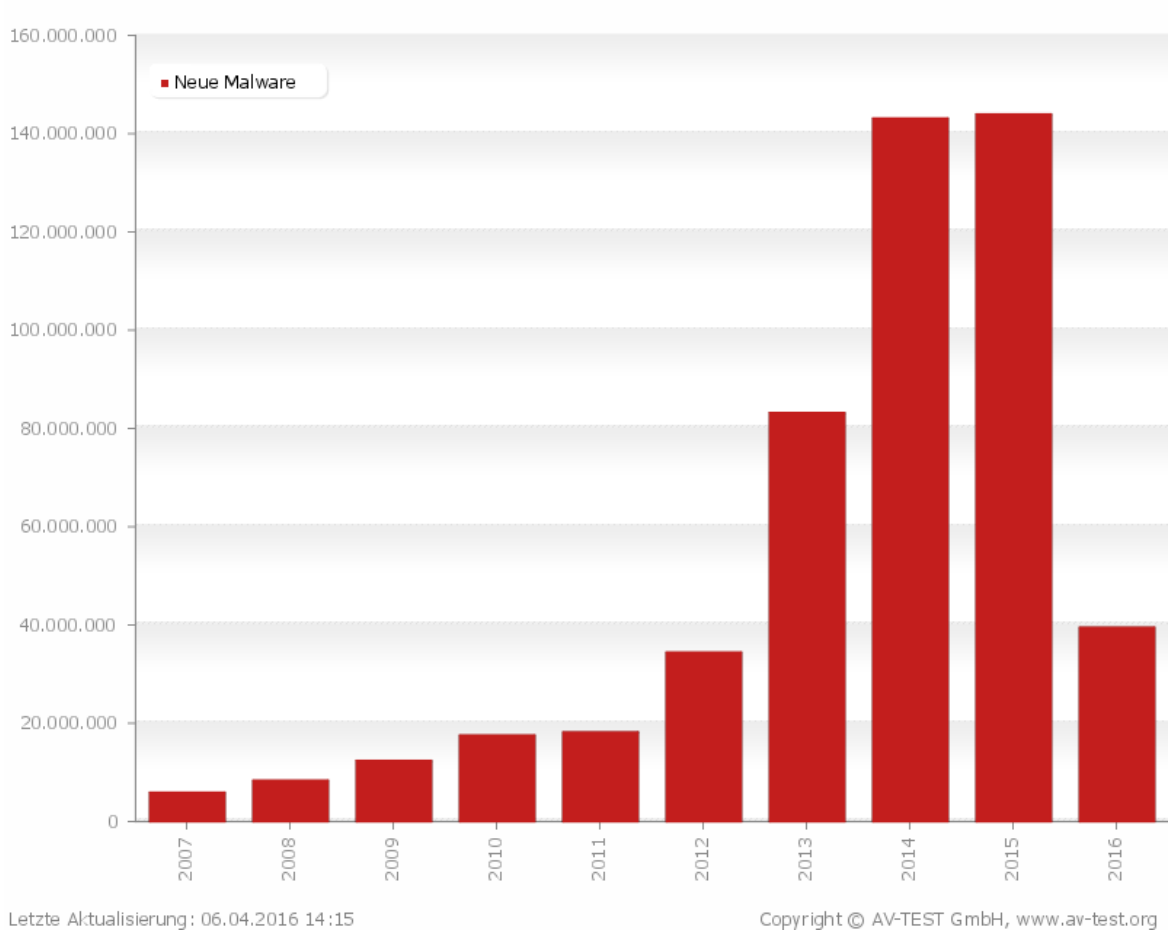
Statistik

Gesamte Malware



Statistik

Neue Malware



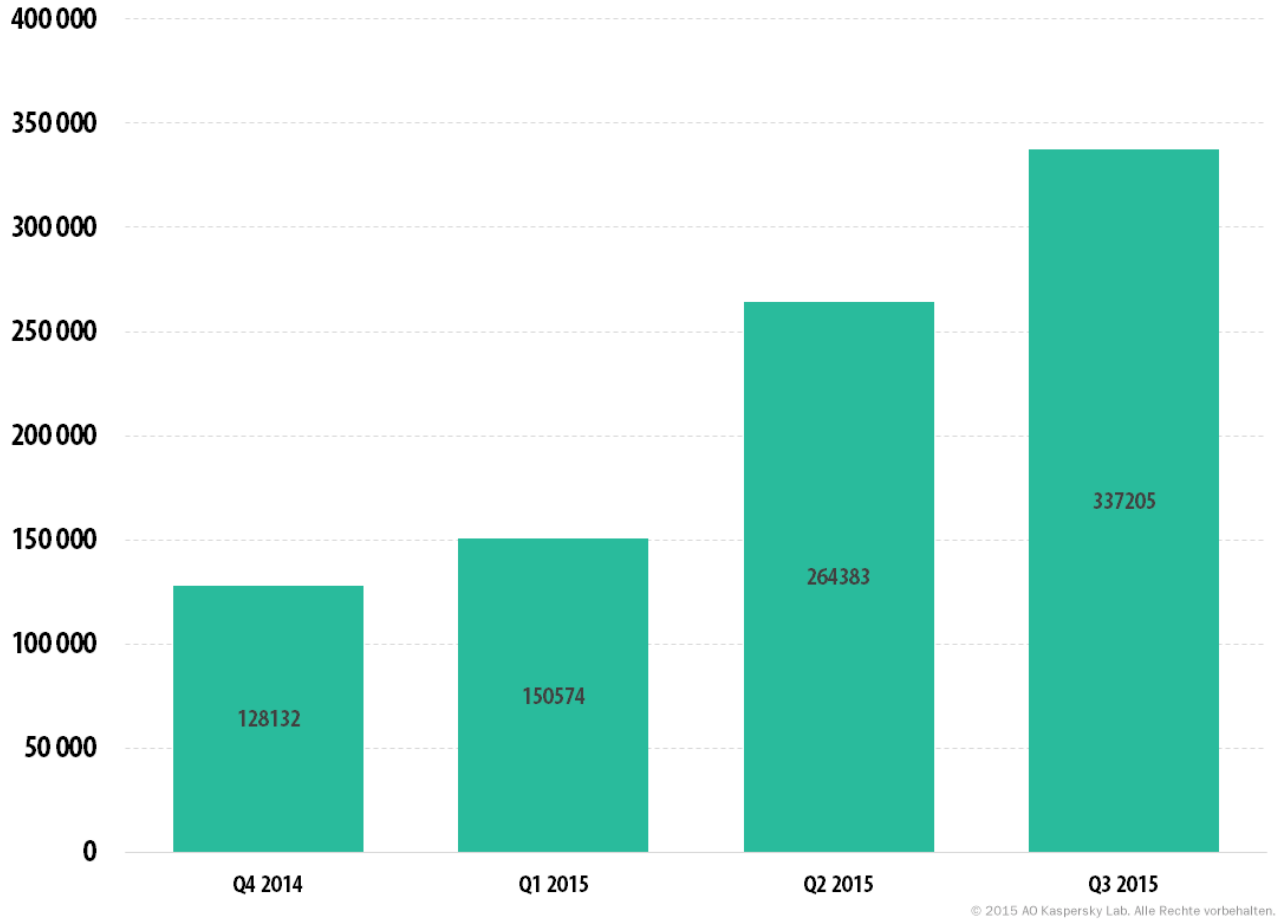
Ransomware

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 Bezahlung eines Lösegelds (ransom).

Statistik

Ransomware



Malware Scanner

Hauptkriterien

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

Erkennungsrate vs. Infektionswahrscheinlichkeit

Infektionswahrscheinlichkeit != 1 - Erkennungsrate

Infektionswahrschinlichkeit bei n voneinander unabhängigen Angriffen:

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

Performance-Effectivity-Tradeoff

Hohe Effektivität $\rightarrow$ hoher Leistungsverbrauch $\rightarrow$ niedrige Performance
Hohe Performance $\rightarrow$ niedriger Leistungsverbrauch $\rightarrow$ 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 zum Zeitpunkt, zu dem das Update an User ausgeliefert wird, sind deren Geräte der neuen Malware schutzlos ausgeliefert.

Anwendungsbeispiel

Implementierung eines Ransom-Trojaners

- Implementierung in Java mit JavaFx Oberfläche
- Täuscht vor, einen Ordner zu optimieren/zu cleanen
- Verschlüsselt Daten im gewählten Ordner
- Verschlüsselung mit Vigenère-Cipher
- Entschlüsselung mit falschem Schlüssel führt zu erneuter Verschlüsselung
- Entschlüsselungs-Key gegen Bezahlung erhältlich

Vielen Dank für eure Aufmerksamkeit