Malware

Inhalt

Themen:

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

Statistik

Neue Malware

bilder/growth.png

Statistik

Gesamte Malware

bilder/total.png

Statistik

Ransomware

bilder/ransom.png

Hauptkriterien:

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

Erkennungsrate vs. Infektionswahrscheinlichkeit

Infektionswahrscheinlichkeit != 1 - Erkennungsrate

Infektionswahrschinlichkeit bei n voneinander unabhngige Angriffe:

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

Performance-Effectivity-Tradeoff

Hohe Effektivitt -> hoher Leistungsverbrauch -> niedrige Performance
Hohe Performance -> niedriger Leistungsverbrauch -> niedrige Effektivitt
Kompromiss zwischen Performance und Effektivitt

Malware Scanning

Static Scanning

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

Malware Scanning

Vorteile

- Erkennt Malware mit festgelegter Signatur garantiert
- Datei muss nicht geffnet/ausgefhrt werden

Nachteile

- bersieht unbekannte Schdlinge
- Erkennt keine alternativen Versionen
- Erkennt nur exakte Treffer
- Speicherverbrauch fr Datenbank

Malware Scanning

Dynamic Scanning

1. Verhalten in Verhaltenskatalog gespeichert
2. berprft Verhalten bei ffnen/Ausfhren
3. Vergleicht Verhalten mit Katalog
4. Blockiert Programm oder lsst Ausfhrung zu

Malware Scanning

Vorteile

- Unbekannte Malware kann erkannt werden

Nachteile

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

Malware Scanning

Heuristic/Proaktive Scanning

- Bestimmt Wahrscheinlichkeit schdlichen Verhaltens
- Fhrt Datei nicht aus
- blockiert Programm aufgrund berechneter Wahrscheinlichkeit

Scanner umgehen

Malware kann nur gefunden werden wenn:

- Signatur in der Datenbank existiert
- Verhalten in der Datenbank existiert
- Heuristische Untersuchung eine hohe Wahrscheinlichkeit fr schdliches Verhalten ermitteln

Design neuer Malware:

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

Schlussfolgerung

Gute Scanner muss:

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

Trotz der Erfllung dieser Voraussetzungen sitzen Malware Entwickler immer am Ingeren Ast. Wird eine Komplett neuartige Malware entwickelt, muss diese erst identifiziert, sowie Regeln und Signaturen dafr erstellt werden. Bis zu dem Zeitpunkt, zu dem das Update an User ausgeliefert wird, sind deren Gerte der neuen Malware Schutzlos ausgeliefert