Proseminar

Secure Computing: Unsichere und weniger Unsichere Systeme

Intrusion Detection

Virenscanner

Philip Daubmeier

31.01.2008

Inhalt

- Virenscanner Arten
- Viren, Erkennung und Entfernung
  - Virentypen
    - Verschlüsselte Viren
    - Metamorphe Viren
  - Erkennung
    - Signaturscanning
    - Transformation
    - Prävention
    - Heuristische Erkennung
    - System Überwachung
  - Entfernung
- Bestmöglicher Schutz
- Was erwartet uns noch?

Virenscanner Arten

- Echtzeit Scanner (Realtime Scanner)
- Festplatten Scanner (On-Demand Scanner)
- Online Scanner

Virentypen

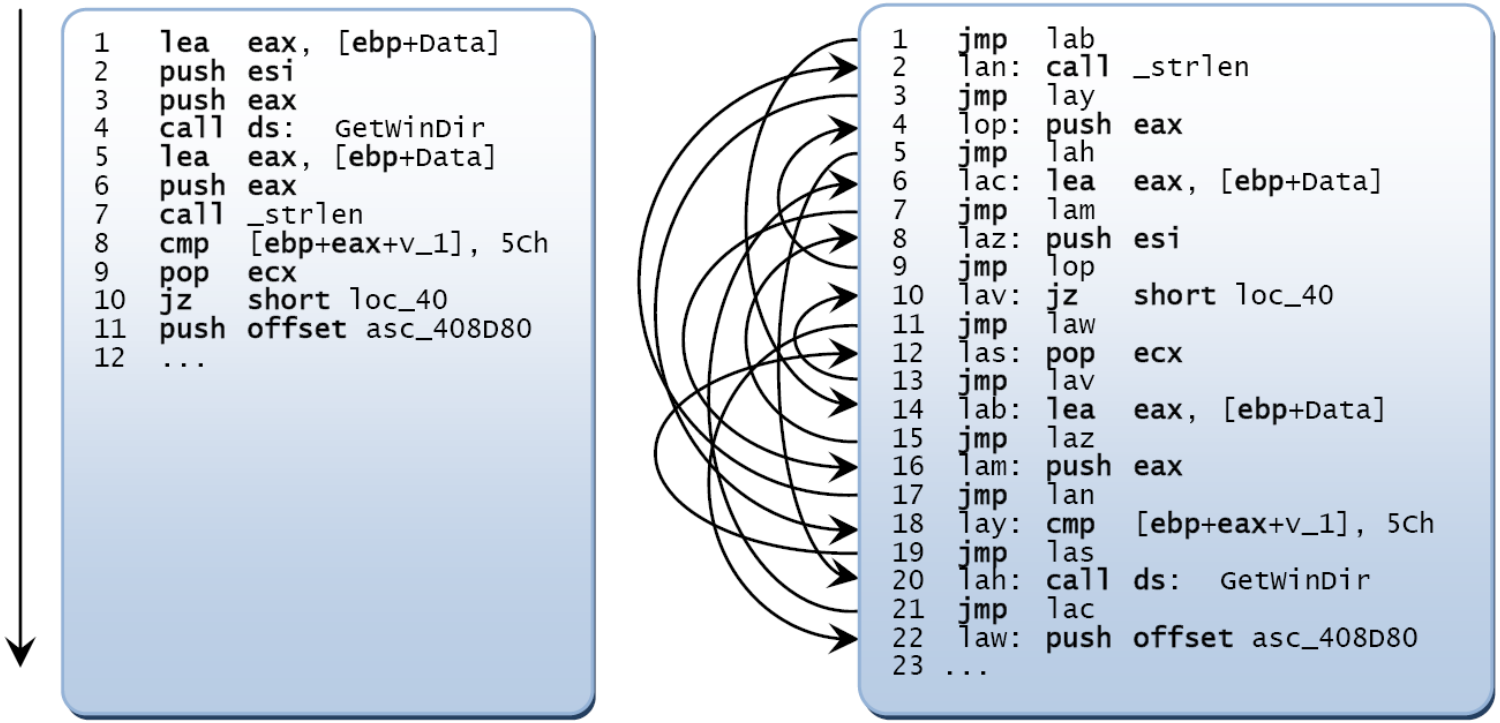
- Verschlüsselte Viren
  - Oligomorphe Viren
  - Polymorphe Viren
- Metamorphe Viren

Virentypen

- Techniken metamorpher Viren
  - Junk Code Insertion
  - Maschinenregister Umbelegung

Virentypen

– Sprungsetzung:

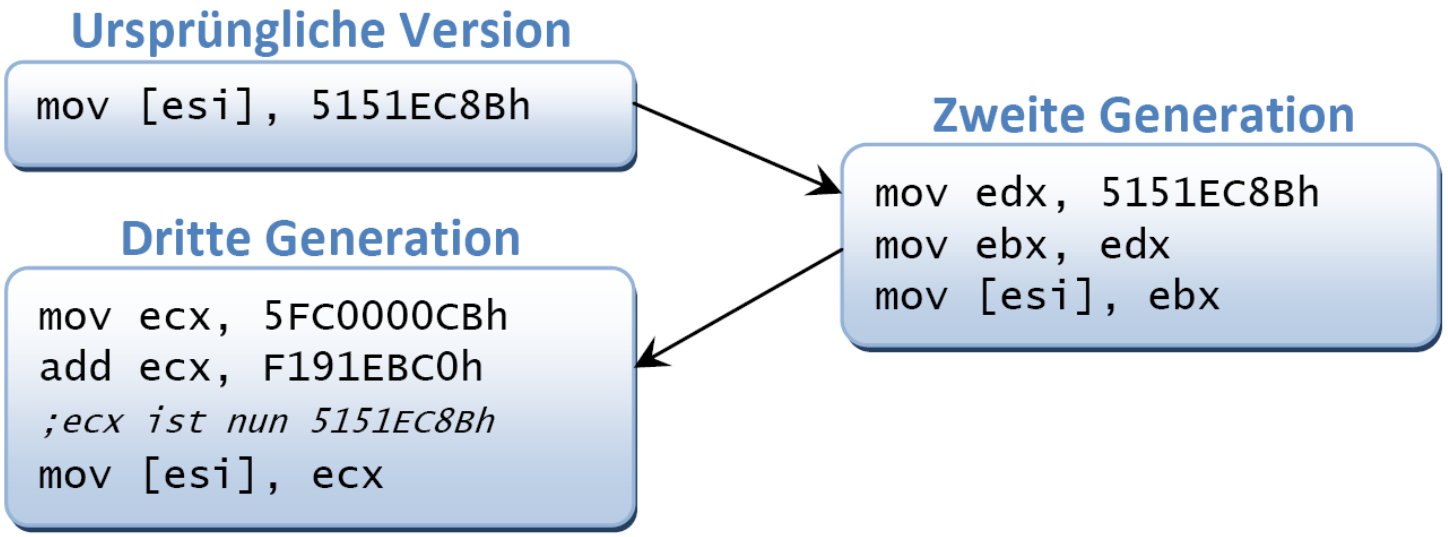


```
1   lea   eax, [ebp+Data]
2   push  esi
3   push  eax
4   call  ds:  GetWinDir
5   lea   eax, [ebp+Data]
6   push  eax
7   call  _strlen
8   cmp   [ebp+eax+v_1], 5Ch
9   pop   ecx
10  jz    short loc_40
11  push  offset asc_408D80
12  ...
```

```
1   jmp   lab
2   lan:  call  _strlen
3   jmp   lay
4   lop:  push  eax
5   jmp   lah
6   lac:  lea   eax, [ebp+Data]
7   jmp   lam
8   laz:  push  esi
9   jmp   lop
10  lav:  jz    short loc_40
11  jmp   law
12  las:  pop   ecx
13  jmp   lav
14  lab:  lea   eax, [ebp+Data]
15  jmp   laz
16  lam:  push  eax
17  jmp   lan
18  lay:  cmp   [ebp+eax+v_1], 5Ch
19  jmp   las
20  lah:  call  ds:  GetWinDir
21  jmp   lac
22  law:  push  offset asc_408D80
23  ...
```

Virentypen

– Konstanten verbergen:



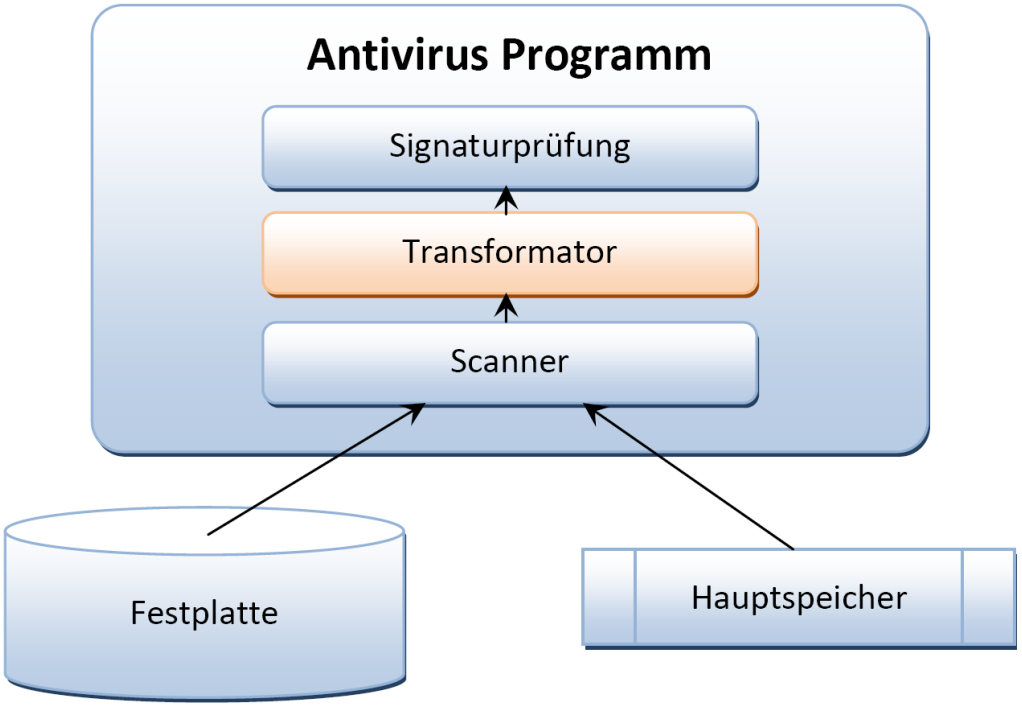
– Einstiegspunkt verbergen

Erkennung

- Signaturscanning
  - Code wird mit Signaturen verglichen
  - Vorteile:
    - Schnell
    - Relativ sichere Erkennung
  - Nachteile:
    - Datenbank muss aktuell gehalten werden
    - Signaturen für jeden Virus nötig

Erkennung

- Transformation
  - Gegen metamorphe Viren



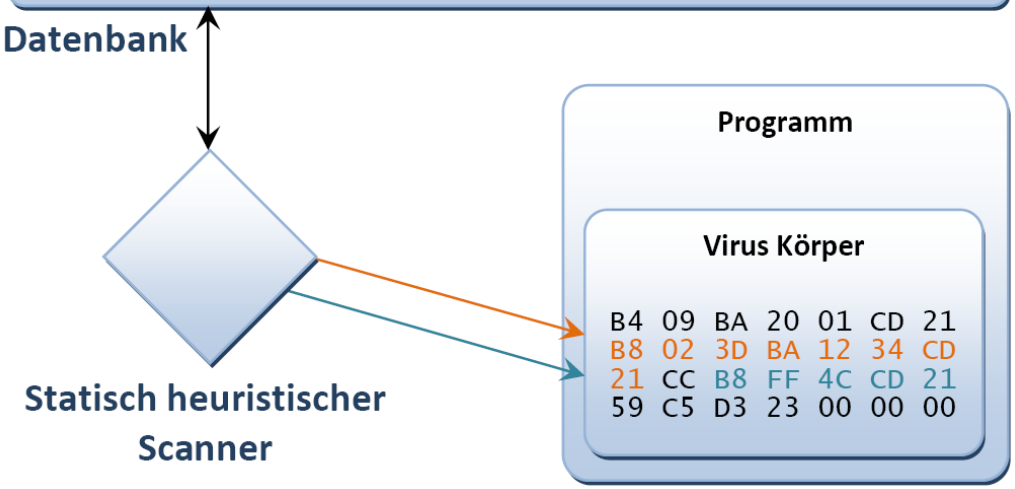
Erkennung

- Prävention
  - Prüfsummen
    - MD5 oder SHA-1 Prüfsummen werden gespeichert
    - Änderung am Programm fällt sofort auf
  - Impfung

Erkennung

- Heuristische Erkennung
  - Statischer heuristischer Scanner

#	Byte Sequenz	Zugewiesenes Verhalten
1.	B8 ?? 4C CD 21	Programm beenden (Permutation 1)
2.	B4 4C CD 21	Programm beenden (Permutation 2)
3.	B4 4C B0 ?? CD 21	Programm beenden (Permutation 3)
4.	B0 ?? B4 4C CD 21	Programm beenden (Permutation 4)
...		
100.	B8 02 3D BA ?? ?? CD 21	Datei öffnen (Permutation 1)
101.	BA ?? ?? B8 02 3D CD 21	Datei öffnen (Permutation 2)
...		



Erkennung

- Dynamischer heuristischer Scanner
  - Virtuelle Maschine
  - Überwacht Systemaufrufe
  - Jedoch: relativ leicht zu umgehen
- Analyse der Verhaltensmuster
  - Expertensystem bewertet Programm
- Vorteile:
  - Auch unbekannte Viren werden gefunden
- Nachteile:
  - Findet keine Anti-Heuristik Viren

Erkennung

- Systemüberwachung
  - Windows Registry
  - Systemvariablen

Entfernung

- Regeln für Entfernung
  - Werden bei Virenscanner Update aktualisiert
  - Müssen für jeden Virus angefertigt werden
- Falls keine Entfernung möglich
  - Quarantäne
  - Overwrite Viren beschädigen Programm

Bestmöglicher Schutz

- Aktuelle Signaturdatenbank
- Backups
- Im Falle einer Infektion:
  - Live CD mit Online Scan
- Programme aus sicheren Quellen beziehen
- 100% Schutz nicht möglich

Was erwartet uns noch?

- Neue Anti-Heuristik Viren
  - Verändertes Verhalten, unauffällige Verbreitung
- Intelligente Hochsprachen Viren
  - Eventuell hochgradig selbstverändernd
  - In Verbindung mit neuesten Rootkits
- Neuronale Netze für Virenscanner
  - Lernender Virenscanner
  - Digitales Immunsystem

Vielen Dank für die Aufmerksamkeit!