MALWARE

AM BEISPIEL VON STUXNET

IAV10/12

Jan Heimbrodt

24.05.2011

Inhalt

1. Definition
   Was ist Malware?
2. Kategorisierung von Malware
   Viren, Würmer, Trojaner, …
3. Was macht Systeme unsicher?
   Angriffsziele, typische Einfallsstore
4. Gegenmaßnahmen
   Was wird gegen Malware unternommen?
5. Stuxnet
   Aufbau, Hintergründe

1. Definition

- Malicious Software (zu Deutsch: bösartige Software)
- Software, die ohne Zustimmung oder Kenntnis des Benutzers schädliche Funktionen ausführt
- in der Regel getarnt oder ganz unsichtbar

2. Kategorisierung von Malware

- Viren
  - infizieren Datei, indem Schadcode hineinkopiert wird
  - passiv, d.h. Interaktion des Benutzers ist notwendig
  - versuchen weitere Dateien zu infizieren

- Würmer
  - kein Wirtsprogramm notwendig
  - verbreiten sich eigenständig
  - nutzen Systemlücken zur Verbreitung

2. Kategorisierung von Malware

- Trojaner
  - als harmlose Software getarnt
  - auf Ausführung durch den Nutzer angewiesen
  - dienen oft als „Container“ für andere Malware

- Spyware
  - Ausspionieren von Nutzerverhalten, Tastatureingaben
  - Daten werden an Urheber übermittelt

2. Kategorisierung von Malware

- Bots
  - Abkürzung von Robot
  - werden von Angreifer ferngesteuert
  - bilden sog. Botnetze:

C&C	P2P
• Zentraler *Command-and Control*-Server • Befehle werden z.b. über IRC erteilt	• Bots sind gleichberechtige Server oder Clients • Schwer lahm zu legen oder Angreifer zu identifizieren

  - werden als „Service“ an Spammer und an DDoS-Angreifer „vermietet“

3. Was macht Systeme unsicher?

- RPC – Remote Procedure Calls
  - Funktionen auf entferntem Rechner aufrufen
- Buffer Overflows
  - Ursache sind häufig Fehler in der Programmierung
  - durch geschicktes Ausnutzen werden Rücksprungadressen mit Code überschrieben

3. Was macht Systeme unsicher?

- JIT-Kompilierung
  - Programmcode wird zur Laufzeit übersetzt
  - Während des Kompilierens wird Code eingeschleust
- Browser und installierte Plug-ins
  - Durch die schnelle Entwicklung immer beliebteres Einfallstor (z.b. ActiveX)
- Last but not least: der Mensch selbst

4. Gegenmaßnahmen

- Verbesserte Compiler
  - Schutzmechanismen werden beim Compiliervorgang in den Code eingebaut
- ASLR – Adress Space Layout Randomization
  - Speicher wird zufällig zugewiesen
  - Programmsprünge sind nicht vorhersehbar

4. Gegenmaßnahmen

- CPUs mit NX-Bit
  - Unter Windows DEP – Data Execution Prevention
  - OS setzt Datenbereiche im Speicher auf No Executable
  - wird dort Code ausgeführt → Hardware-Interrupt
  - Kein Schutz vor Buffer Overflows

- Browser
  - Sandboxing, Phishing-Schutz, Updates

4. Gegenmaßnahmen

- Honeypots
  - Bewusst unsichere Systeme
  - „sammeln“ Malware zur Erkennung & Analyse von Angriffsmethoden und –mustern
- Firewalls/Virenscanner
- Faktor Mensch
  - Bewusstsein für Sicherheit muss entwickelt werden

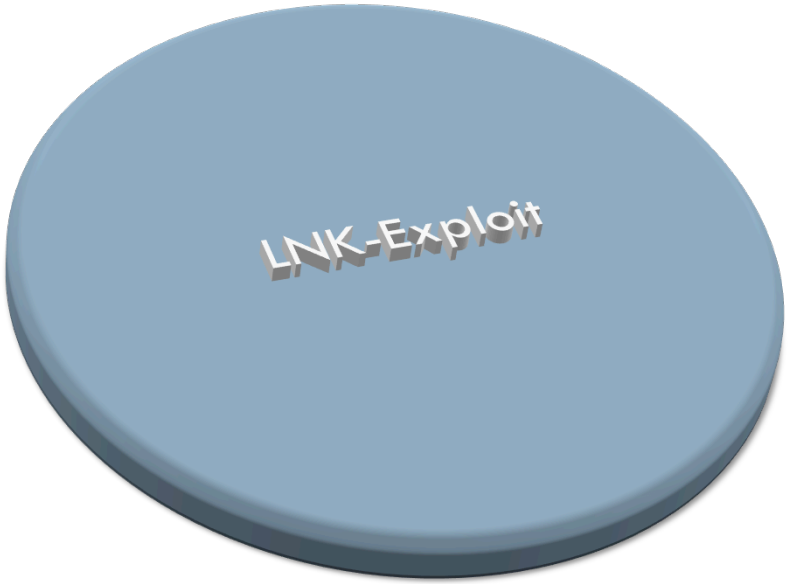
5. Stuxnet

- Im Juni 2010 entdeckter Computerwurm
- Sehr komplexe und robuste Malware
- Spionage/Manipulation von SCADA-Systemen
  - Supervisory Control and Data Acquisition
  - Dient der Prozessüberwachung von Industrieprozessen

5. Stuxnet - Infektion

- Nutzt 4 Zero-Day Exploits
  - LNK-Exploit
  - Lücke in der Anzeige von Dateiverknüpfungen
  - Shell will Icon der Zieldatei per Systemfunktion nachladen
  - Code kann ausgeführt werden
  - 100% zuverlässig unter Win2000 bis Win 7

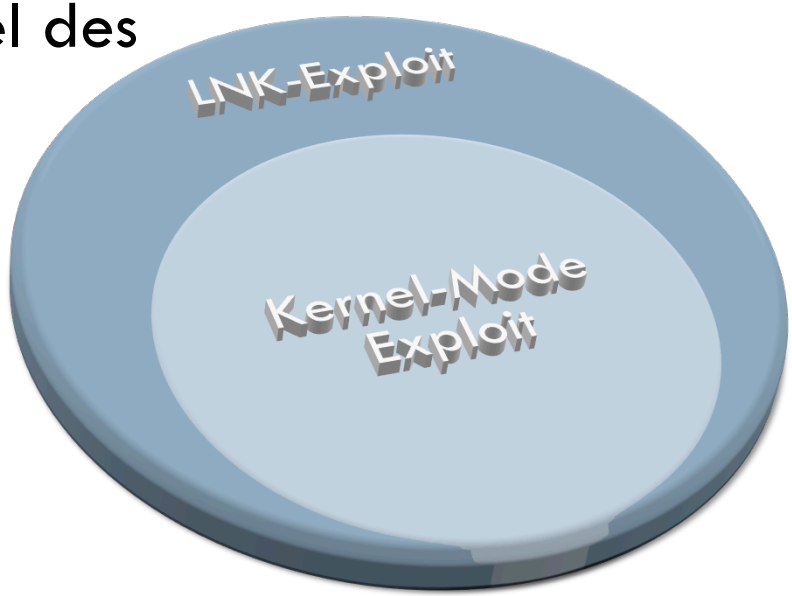
  → Angreifer hat Zugriff auf das System mit Userrechten



5. Stuxnet - Infektion

- Nutzt 4 Zero-Day Exploits
  - Kernel-Mode Exploit win32k.sys
  - Kerneltreiber wird mit Hilfe von gestohlenen Zertifikaten im Hintergrund manipuliert
  - Schadcode wird beim Wechsel des Keyboard-Layouts ausgeführt
  - 100% zuverlässig unter Win2000 bis WinXP SP2

  → System-Berechtigungen



5. Stuxnet - Infektion

- Nutzt 4 Zero-Day Exploits
  - Task Scheduler Exploit
  - Tasks werden in XML-Datei (schreib-/lesbar) angelegt
  - Schadcode wird angehängt
  - File-Checksum wird manipuliert
  - Code läuft mit dem Task
  - 100% zuverlässig unter

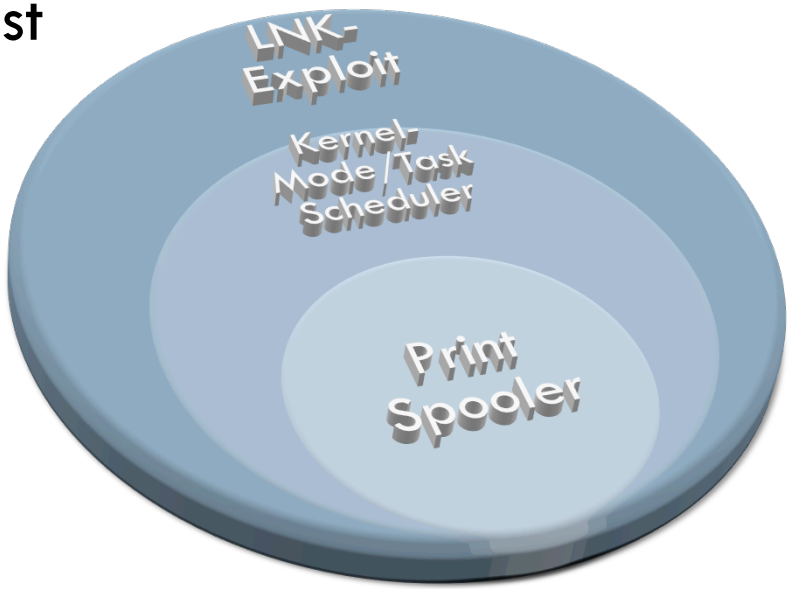
    unter Win Vista bis Win 7

    → System-Berechtigungen

5. Stuxnet - Infektion

- Nutzt 4 Zero-Day Exploits
  - Print Spooler RFC Lücke
  - Über Druckerfreigaben werden Dateien auf entfernten Rechnern in beliebigen Ordnern erstellt
  - Rechner verbinden sich als Gast
  - „Drucken in Datei“
  - Drucken erfolgt unter XP mit System-Rechten

  → Weiterverbreitung im LAN



5. Stuxnet - Schadroutine

- Infizierte Rechner werden nach Installationen von STEP7/WinCC durchsucht
  - STEP7 dient der Programmierung von SPS-Bausteinen
  - WinCC dient der Prozessvisualisierung
- Programmbibliotheken werden infiziert
- SPS-Bausteine können, unsichtbar für Personal, manipuliert werden

Quelle: http://de.wikipedia.org/wiki/SIMATIC_S7 User: Ulli1105

5. Stuxnet – Urheber und Ziele

- Aufgrund seiner Komplexität stammt der Wurm wahrscheinlich von einer Regierungsstelle
- Verschiedene Indizien im Code deuten auf USA/ Israel als Urheber
- Mögliches Ziel waren Atomanlagen/das Atomprogramm des Iran

Quellen

- http://de.wikipedia.org/wiki/Malware
- http://de.wikipedia.org/wiki/Computervirus
- http://de.wikipedia.org/wiki/Computerwurm
- http://de.wikipedia.org/wiki/Trojanisches_Pferd_(Computerprogramm)
- http://de.wikipedia.org/wiki/Spyware
- http://de.wikipedia.org/wiki/Bot
- http://de.wikipedia.org/wiki/Remote_Procedure_Call
- http://de.wikipedia.org/wiki/Puffer%C3%BCberlauf
- http://de.wikipedia.org/wiki/Exploit
- http://de.wikipedia.org/wiki/Just-in-time-Kompilierung
- http://de.wikipedia.org/wiki/ASLR
- http://de.wikipedia.org/wiki/NX-Bit
- http://de.wikipedia.org/wiki/Honeypot
- http://de.wikipedia.org/wiki/Stuxnet
- http://de.wikipedia.org/wiki/Supervisory_Control_and_Data_Acquisition
- http://events.ccc.de/congress/2010/Fahrplan/events/4245.en.html