Viren und Würmer

B. Mayer, M. Moser, M. Schönegger

WAP (WS 2016/17)

Inhalt

Malware

- "Malicious Software"
- Unter den Aspekt Malware fallen folgende Bereiche:
  - Viren, Würmer,
  - Trojanische Pferde, Dialer,
  - Adware, Spyware, ...
- Wer erstellt Malware?
  - Programmierer mit sehr guten Betriebssystem Kenntnissen
  - sogenannte Virengeneratoren
- werden Viren und Würmer genauer betrachten

Viren

- Begriff Viren meist als Oberbegriff Malware verwendet (Stichwort Anti-Viren-Software)
- nutzen Autorisierung von Programmen im Betriebssystem
- keine selbständigen Programmroutinen
- integrieren Programmcode in Dateien

Verbreitung von Viren

- **Ziele der Verbreitung**:
  - Ausführung von Schadcode bei bestimmten Aktionen des Nutzers
  - Eindringen in andere Ressourcen des Computers
- **Art der Verbreitung:**
  - Virus kopiert sich auf Wechseldatenträger und infiziert Dateien
  - Nutzer versendet eine E-Mail mit infiziertem Anhang

Verschiedene Arten der gängigsten Viren

1. Bootviren
2. Dateiviren
   - Überschreiben des Dateiinhalts
   - Parasitäre Viren
   - Compagnion Viren
   - Stealth Viren
   - Script Viren
3. Multipartite Viren

Bootviren

- befinden sich im Bootsektor des Systems
- kommen seltener vor, sind aber zerstörerischer
- systemnaher Bezug erleichtert zuverlässige Ausführung
- auch auf CDs und USB-Sticks möglich

Dateiviren

- nutzen Dateisystem zur Vervielfältigung
- Eindringen auf unterschiedliche Art und Weise in ausführbare Dateien
- erstellen Kopien in Verzeichnissen
- nutzen Organisationsstruktur des Dateisystems

Dateiviren

- **Überschreiben des Dateiinhaltes:**
  - einfachste Methode
  - ersetzen Code der Datei durch eigenen Code
  - schnell erkennbar

Dateiviren

- **Überschreiben des Dateiinhaltes:**
  - einfachste Methode
  - ersetzen Code der Datei durch eigenen Code
  - schnell erkennbar
- **Parasitäre Viren:**
  - am weitesten verbreitet
  - fügen Code in Dateien ein und verändern deren Inhalt

Dateiviren

- **Überschreiben des Dateiinhaltes:**
  - einfachste Methode
  - ersetzen Code der Datei durch eigenen Code
  - schnell erkennbar
- **Parasitäre Viren:**
  - am weitesten verbreitet
  - fügen Code in Dateien ein und verändern deren Inhalt
- **Compagnion Viren:**
  - ändern den Inhalt einer Datei überhaupt nicht
  - erstellen eine Doppelgänger-Datei mit ihrem Code
  - beim Öffnen der Datei erhält Doppelänger-Datei die Kontrolle

Dateiviren

- **Stealth Viren:**
  - sind spezielle Tarnviren
  - bei Analyse von Anti-Viren-Programm wird Code entfernt
  - nach Beendigung wird Code wieder eingefügt

Dateiviren

- **Stealth Viren:**
  - sind spezielle Tarnviren
  - bei Analyse von Anti-Viren-Programm wird Code entfernt
  - nach Beendigung wird Code wieder eingefügt
- **Script Viren:**
  - werden mithilfe von Script Sprachen geschrieben
  - infizieren andere Script Programme oder
  - sind Bestandteil von Viren, welche mehrere Komponenten enthalten
  - können andere Formate wie z.B: HTML infizieren

Würmer

[4]

- nutzen im Gegensatz zu Viren Infrastruktur eines Netzwerkes
- benötigen kein Wirtsprogramm
- wesentliches Unterscheidungsmerkmal ist Verbreitungsmethode
- Unterscheidung nach Art des Eindringens in ein System

Würmer

Arten von Würmern

- Emailwürmer
- Würmer in Instant Messengern (IM)
- sonstige Würmer
  - Kopieren auf Netzwerkressourcen
  - Einschleusen über Schwachstellen in Betriebssystemen oder Anwendungen
  - Eindringen in öffentlich zugängliche Netzwerkressourcen

Berühmte Würmer

1971: erstes wurmähnliches Programm: **Creeper** (Tenex)

Berühmte Würmer

1971: erstes wurmähnliches Programm: **Creeper** (Tenex)

$\Rightarrow$ erster Nematode: **Reaper**

Berühmte Würmer

1971: erstes wurmähnliches Programm: **Creeper** (Tenex)

$\Rightarrow$ erster Nematode: **Reaper**

1988: erster Internetwurm: **Morris Worm** (Sun, VAX)

Berühmte Würmer

1971: erstes wurmähnliches Programm: **Creeper** (Tenex)
$\Rightarrow$ erster Nematode: **Reaper**

1988: erster Internetwurm: **Morris Worm** (Sun, VAX)

2003: **SQL Slammer** aka **Sapphire Worm** $\rightarrow$ 2 (Microsoft SQL Server) - schnellste Verbreitung

2004: **Sasser** (Windows) - in Deutschland entstanden

Berühmte Würmer

1971: erstes wurmähnliches Programm: **Creeper** (Tenex)
$\Rightarrow$ erster Nematode: **Reaper**

1988: erster Internetwurm: **Morris Worm** (Sun, VAX)

2003: **SQL Slammer** aka **Sapphire Worm** $\rightarrow 2$
(Microsoft SQL Server) - schnellste Verbreitung

2004: **Sasser** (Windows) - in Deutschland entstanden

2010: gezielte Sabotage von Industrieanlagen: **Stuxnet** $\rightarrow 3$
(Windows, Siemens)

2012: Spionage: **Flame** (Wurm/Trojaner, 20 MB)

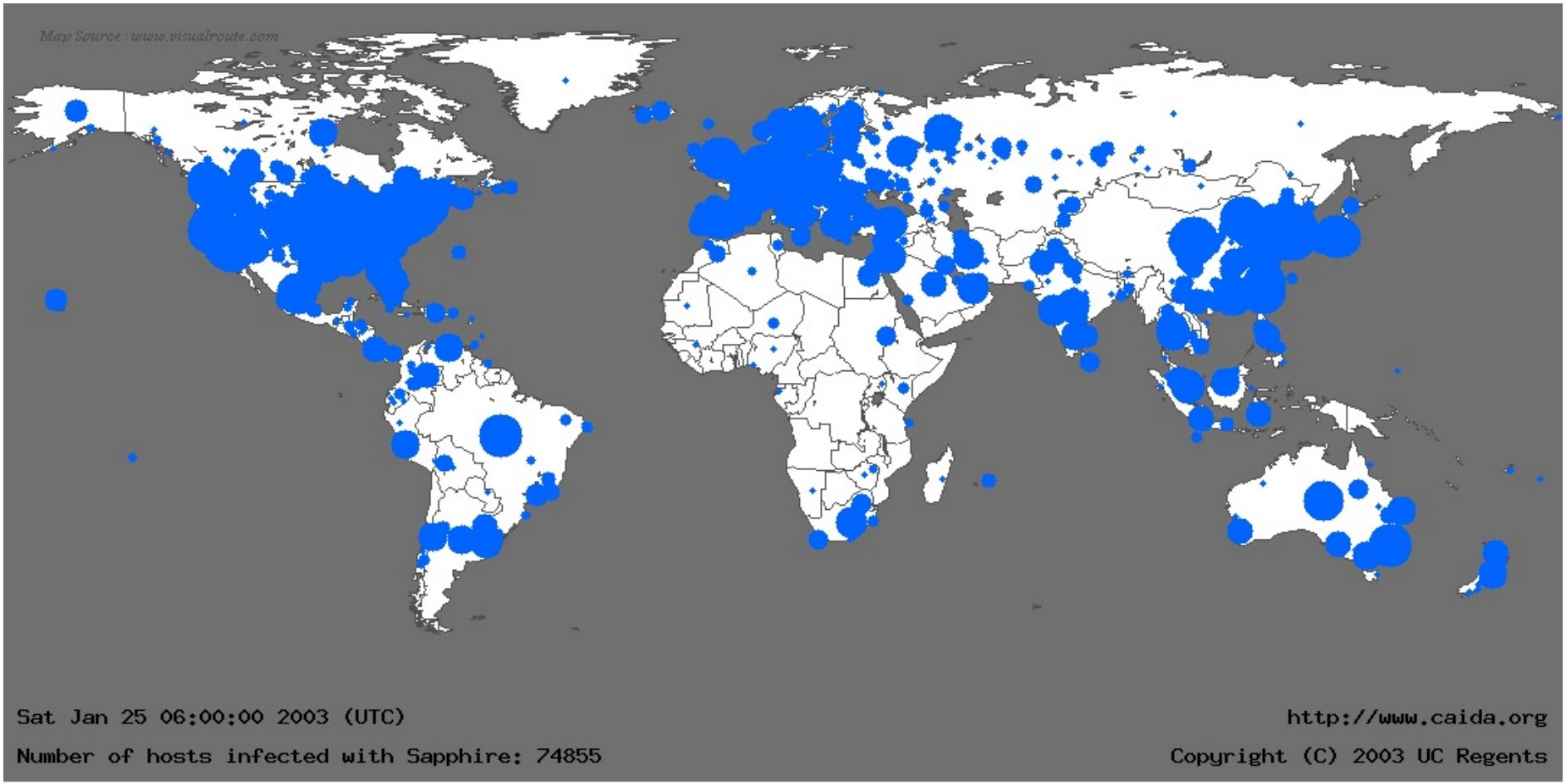
Slammer (Wurm)

- klein, schnell, einfach
- erster Ausbruch: 25. Jänner 2003
- hauptsächlich betroffene Systeme:
  - Microsoft SQL-Server
  - MSDE 2000
- x86 Assembler
- User Datagram Protocol (UDP)

User Datagram Protocol - kurze Erklärung

- Versand von Datagrammen in IP-basierten Rechnernetzen
- minimal, verbindungslos, unzuverlässig, ungesichert
- Daten werden schnell hintereinander versendet
- maximale Größe: 65535 Bytes ($2^{16} - 1$ Bytes adressierbar)
- verwendet z.B. für:
  - Voice over IP (VoIP)
  - Domain Name System (DNS)
  - Dynamic Host Configuration Protocol (DHCP)

Slammer - Verbreitung



[3]

Slammer - Verbreitung

1. Eintritt
2. Neuprogrammierung
3. zufälliges Ziel
4. Vervielfältigung
5. Wiederholung

1. Eintritt

- getarnt als UDP-Paket
- übertragener String länger als 128 Byte (SQL-Anfrage)
- geschickt programmiert, sodass Ende von SQL Statement übersprungen wird
- Bufferoverflow

2. Neuprogrammierung

- Sicherheitslücke ausnützen und eigenen Code einschleusen
- ein Teil des Stacks wird überschrieben
- Code wird unbemerkt ausgeführt

3. Zufälliges Opfer

- generiert zufällige IP-Adresse
- Zeit in Millisekunden seit dem Systemstart als Grundlage für die Zufalls-IP
- mögliches Ziel ist jeder Computer im Internet

4. Vervielfältigung

- Slammer erstellt eine Kopie seines eigenen Codes
- vom infizierten Computer aus wird diese nun als UDP-Paket getarnt versendet
- 70 Millionen Anfragen / Sekunde

5. Wiederholung

- sofortige Wiederholung der Schritte
- neue Zufallszahl wird durch Bit-Shift-Operationen erzeugt ($\rightarrow$ Wiederholung von IP-Adressen)
- so schnell, dass sich mehrere Instanzen von Slammer die Bandbreite teilen müssen ($\rightarrow$ langsamere Ausbreitung)

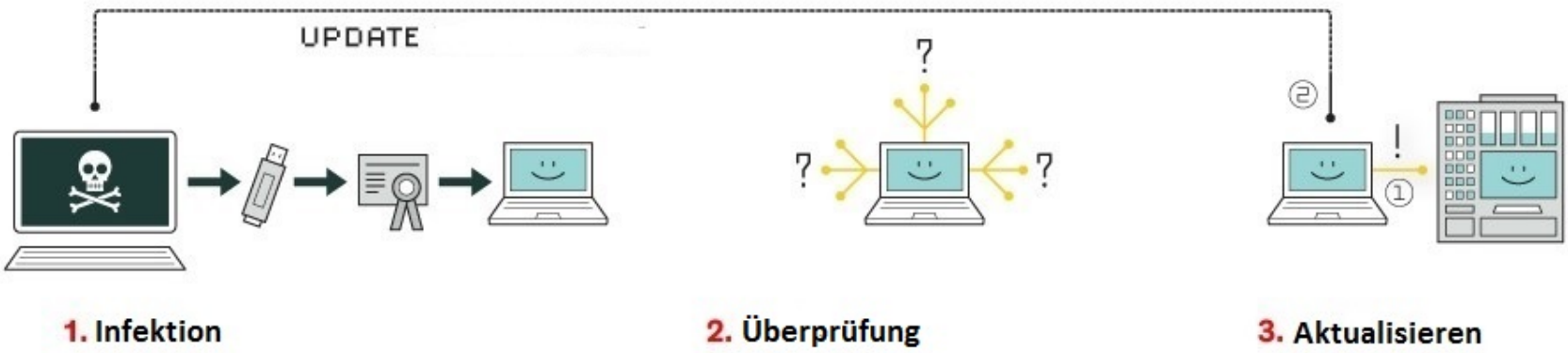
Gegenmaßnahmen

- Blockieren von Port 1434 (UDP)
- Neustart des Computers (Slammer liegt im RAM)
- Verwendung von aktueller Software

Stuxnet

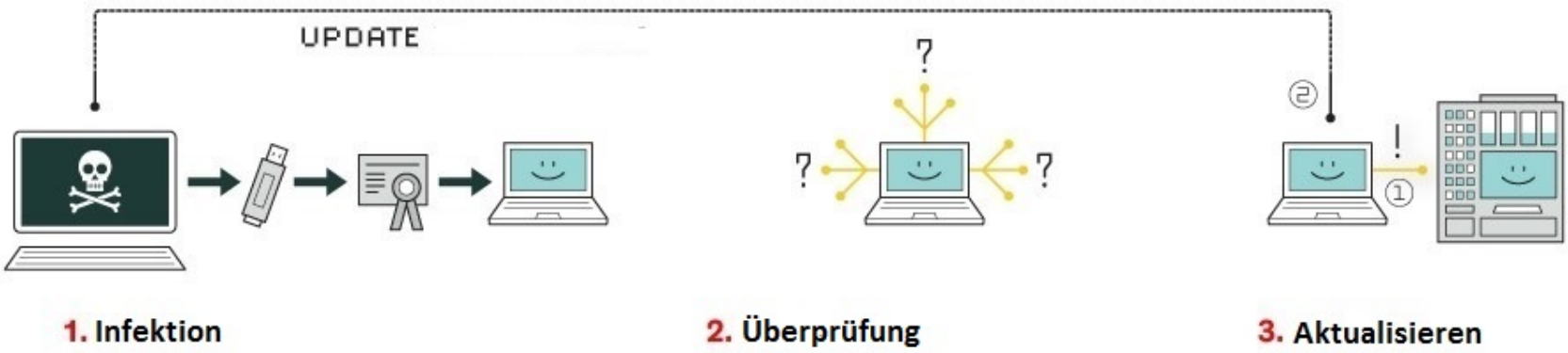
- erstmals entdeckt im Juni 2010
- 500kB Wurm
- genialer Programmcode
- Software von Industrieanlagen im Iran befallen (Zentrifugen in Urananreicherungsanlagen)
- vermutlich staatlich finanziert (USA und Israel)
- Absicht nicht finanziell sondern rein politisch

So funktioniert Stuxnet



cf. [2]

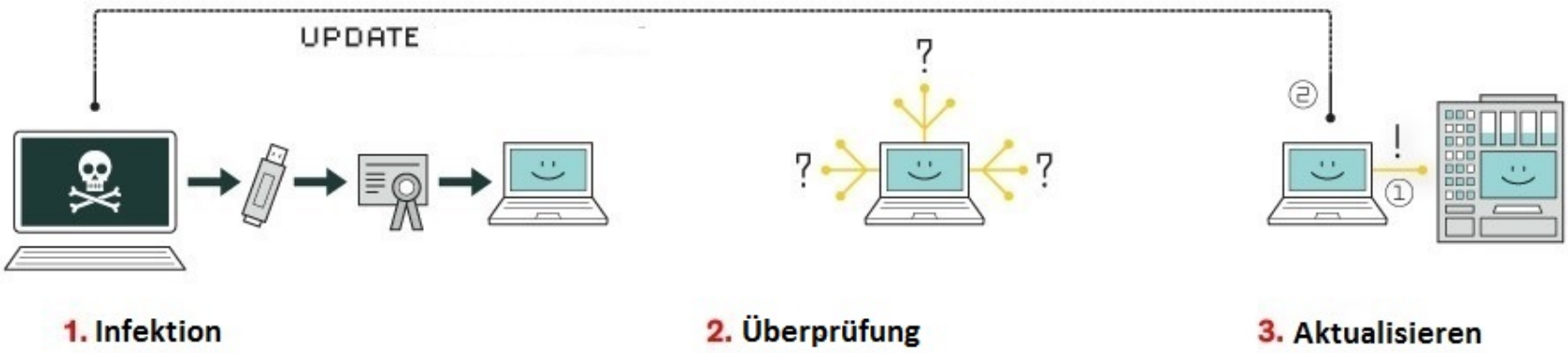
So funktioniert Stuxnet



cf. [2]

1. infiziert Windows-Rechner über USB-Stick (gestohlenes Zertifikat), vervielfältigt sich selbst und verbreitet sich im LAN

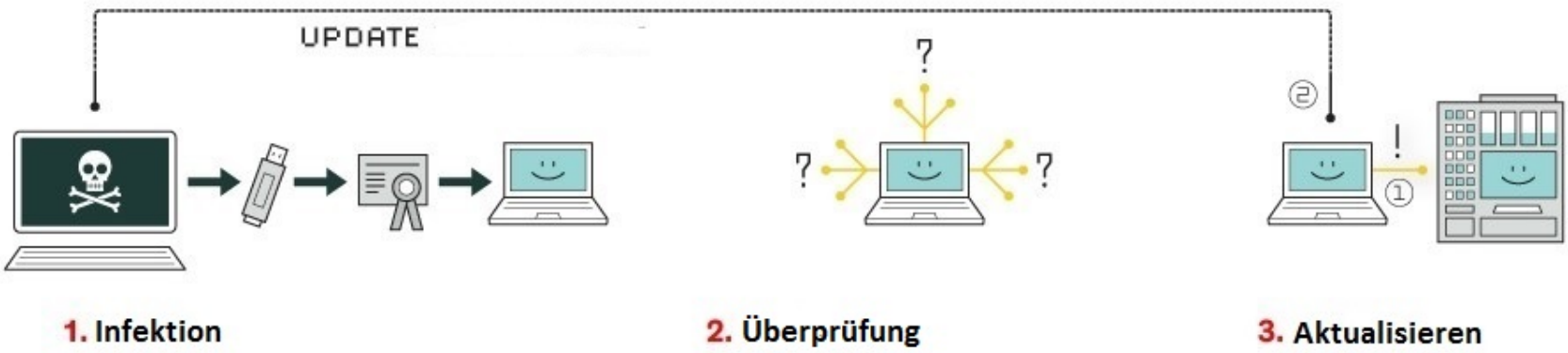
So funktioniert Stuxnet



cf. [2]

1. infiziert Windows-Rechner über USB-Stick (gestohlenes Zertifikat), vervielfältigt sich selbst und verbreitet sich im LAN
2. überprüft, ob der befallene Rechner ein Zielobjekt ist (ob die Siemens Steuerungssoftware Step7 installiert ist)

So funktioniert Stuxnet



cf. [2]

1. infiziert Windows-Rechner über USB-Stick (gestohlenes Zertifikat), vervielfältigt sich selbst und verbreitet sich im LAN
2. überprüft, ob der befallene Rechner ein Zielobjekt ist (ob die Siemens Steuerungssoftware Step7 installiert ist)
3. falls Step7 nicht installiert (1): keine Aktion
   falls Step7 gefunden (2): Update über Internet, weiter bei **4.**

So funktioniert Stuxnet

4. Eingriff

5. Beobachten

6. Vortäuschen und zerstören

cf. [2]

So funktioniert Stuxnet

4. nutzt bisher unbekannte Sicherheitslücken, um die Steuerungssoftware zu befallen

4. Eingriff

5. Beobachten

6. Vortäuschen und zerstören

cf. [2]

So funktioniert Stuxnet

4. nutzt bisher unbekannte Sicherheitslücken, um die Steuerungssoftware zu befallen
5. beobachtet die Steuerung der Zentrifugen und sammelt diese Informationen

4. Eingriff

5. Beobachten

6. Vortäuschen und zerstören

cf. [2]

So funktioniert Stuxnet

4. nutzt bisher unbekannte Sicherheitslücken, um die Steuerungssoftware zu befallen
5. beobachtet die Steuerung der Zentrifugen und sammelt diese Informationen
6. sendet falsche Informationen an die Steuerungssoftware während er die Zentrifugen übersteuert und so zerstört

4. Eingriff

5. Beobachten

6. Vortäuschen und zerstören

cf. [2]

Zero-Day Exploits

Zero-Day Exploit

Ausnutzen einer Schwachstelle oder Sicherheitslücke in einem Programm oder System, bevor das Problem bekannt ist bzw. durch einen Patch behoben werden konnte

Zero-Day Exploits

Zero-Day Exploit

Ausnutzen einer Schwachstelle oder Sicherheitslücke in einem Programm oder System, bevor das Problem bekannt ist bzw. durch einen Patch behoben werden konnte

- Stuxnet verwendete sogar gleich 4 Zero-Day Exploits, die einander perfekt ergänzten:

Zero-Day Exploits

Zero-Day Exploit

Ausnutzen einer Schwachstelle oder Sicherheitslücke in einem Programm oder System, bevor das Problem bekannt ist bzw. durch einen Patch behoben werden konnte

- Stuxnet verwendete sogar gleich 4 Zero-Day Exploits, die einander perfekt ergänzten:
  - LNK-Dateien $\Rightarrow$ Verbreitung via USB-Stick

Zero-Day Exploits

Zero-Day Exploit

Ausnutzen einer Schwachstelle oder Sicherheitslücke in einem Programm oder System, bevor das Problem bekannt ist bzw. durch einen Patch behoben werden konnte

- Stuxnet verwendete sogar gleich 4 Zero-Day Exploits, die einander perfekt ergänzten:
  - LNK-Dateien $\Rightarrow$ Verbreitung via USB-Stick
  - Druckerspooler $\Rightarrow$ Verbreitung in Netzwerken

Zero-Day Exploits

Zero-Day Exploit

Ausnutzen einer Schwachstelle oder Sicherheitslücke in einem Programm oder System, bevor das Problem bekannt ist bzw. durch einen Patch behoben werden konnte

- Stuxnet verwendete sogar gleich 4 Zero-Day Exploits, die einander perfekt ergänzten:
  - LNK-Dateien $\Rightarrow$ Verbreitung via USB-Stick
  - Druckerspooler $\Rightarrow$ Verbreitung in Netzwerken
  - Laden von Tastaturbelegungen $\Rightarrow$ Privileg-Eskalation

Zero-Day Exploits

Zero-Day Exploit

Ausnutzen einer Schwachstelle oder Sicherheitslücke in einem Programm oder System, bevor das Problem bekannt ist bzw. durch einen Patch behoben werden konnte

- Stuxnet verwendete sogar gleich 4 Zero-Day Exploits, die einander perfekt ergänzten:
  - LNK-Dateien $\Rightarrow$ Verbreitung via USB-Stick
  - Druckerspooler $\Rightarrow$ Verbreitung in Netzwerken
  - Laden von Tastaturbelegungen $\Rightarrow$ Privileg-Eskalation
  - Task-Scheduler $\Rightarrow$ Privileg-Eskalation

Zero-Day Exploits

Zero-Day Exploit

Ausnutzen einer Schwachstelle oder Sicherheitslücke in einem Programm oder System, bevor das Problem bekannt ist bzw. durch einen Patch behoben werden konnte

- Stuxnet verwendete sogar gleich 4 Zero-Day Exploits, die einander perfekt ergänzten:
  - LNK-Dateien ⇒ Verbreitung via USB-Stick
  - Druckerspooler ⇒ Verbreitung in Netzwerken
  - Laden von Tastaturbelegungen ⇒ Privileg-Eskalation
  - Task-Scheduler ⇒ Privileg-Eskalation
- Microsoft veröffentlichte Patches noch 2010

Diskussion

1. **Überblick Malware**
   - Viren
   - Würmer
2. **SQL Slammer**
3. **Stuxnet**
4. **Quellenverzeichnis**

E. Kaspersky.
Malware. Von Viren, Würmern, Hackern und Trojanern und wie man sich vor ihnen schützt.
Hanser München, 2008.

D. Kushner.
The Real Story of Stuxnet.
IEEE Spectrum, 26. Feb. 2013.

D. Moore, V. Paxson, S. Savage, C. Shannon, S. Staniford, and N. Weaver.
Inside the Slammer Worm.
IEEE Security and Privacy, (4):33–39, Aug. 2003.

J. Riordan, A. Wespi, and D. Zamboni.
How To Hook Worms.
IEEE Spectrum, 2. Mai 2005.