

# IT-Sicherheit

- Sicherheit vernetzter Systeme -

## Kapitel 1: Einleitung

# Kap. 1: Einleitung: Motivierendes Beispiel

1. Internet Worm
  - Historischer Rückblick
  - Funktionsweise
  - Lessons Learned
  
2. SQL Slammer Wurm
  - Historischer Rückblick
  - Funktionsweise
  - Lessons Learned
  
3. Vergleich von Internet Worm und Slammer
  
4. Stuxnet

# Historischer Rückblick I: 1988 Internet Worm

## ■ Chronologie der Vorfälle an der University of Utah:

- Mittwoch 2. November 1988
  - 17:01:59: Test oder Start des Wurms
  - 17:04: Maschine an der Cornell University „befallen“
  - 20:49: Wurm infiziert VAX 8600 an der Univ. Utah (cs.utah.edu)
  - 21:09: Wurm versucht von VAX aus andere Maschinen zu infizieren
  - 21:21: Load (Anzahl der rechenbereiten Prozesse) von 5
  - 21:41: Load von 7
  - 22:01: Load von 16
  - 22:06: Es können keine Prozesse mehr gestartet werden, Benutzer können sich nicht mehr anmelden
  - 22:20: Systemadministrator terminiert den Wurm Prozess
  - 22:41: Der Wurm ist zurück; Load 27
  - 22:49: System shutdown, reboot
  - 23:21: Der Wurm ist zurück; Load 37

# Internet Wurm: Globale Sicht

## ■ Mittwoch 2. Nov. 1988

- 17:01:59: Wurm Test oder Start
- 21:00: Stanford University; ca. 2500 Unix Maschinen infiziert
- 21:30: MIT infiziert
- 22:54: University of Maryland
- 23:00: University of California, Berkeley
- 24:00: SRI International

## ■ Donnerstag, 3. Nov. 1988

- 2:00: Lawrence Livermore National Laboratory
- 2:28: E-mail Warnung; erreicht aber die meisten nicht vor Samst. 5. Nov. 5:00
  - Wurm infiziert SUN und VAX
  - Beinhaltet DES Tabelle
  - Nutzt `.rhosts` und `host.equiv`
  - Speichert `X*` Dateien in `/tmp`

## □ 5:58: Bug fix posting aus Berkeley:

- Sendmail's `debug` Kommando deaktivieren
- C Compiler umbenennen
- Linker umbenennen

## □ 8:00: Berkely entdeckt `finger` Mechanismus

## □ 10:30: TV Teams am MIT

- Ca. 10 % Infektionsrate am MIT (2000 Maschinen)

## □ 11:00: Titel-Story in den Nachrichten:

- Mehr als 6000 hosts im Internet infiziert (10 %)

# Internet Wurm: „How it Works“

## ■ Wie befällt er neue Maschinen?

- ❑ `sendmail` Bug (seit langem bekannt)
- ❑ `finger` Bug; Buffer Overflow (nur VAX werden befallen)
- ❑ Remote execution (`rsh`, `rexec`)

## ■ Welche Accounts werden angegr.

- ❑ Offensichtliche Passwörter
  - Leeres Passwort
  - Benutzername
  - Benutzername+Benutzername
  - Infos aus GECOS-String
  - Nachname
  - Nachname rückwärts
- ❑ Build-In Wörterbuch (432 Wörter)
- ❑ `/usr/dict/words` (24'474 Wörter)
- ❑ Trusted Host Beziehung (`.rhosts`)

## ■ Welche hosts werden angegriffen?

- ❑ Maschinen in `/.rhosts` und `/etc/host.equiv`
  - ❑ `.forward` Datei gebrochener Accounts
  - ❑ `.rhosts` Datei gebr. Accounts
  - ❑ Gateways aus der Routing-Tabelle
  - ❑ Endpunkte von Point to Point Verbindungen
  - ❑ Zufällig geratene Adressen
  - ❑ Nur Sun und VAX
- ## ■ Was der Wurm NICHT tut:
- ❑ Versuchen root access zu erhalten
  - ❑ Well-known Accounts angreifen
  - ❑ Daten zerstören
  - ❑ „Zeitbomben“ zurücklassen

# Internet Wurm: Programm Struktur

## main Routine

```
argv[0] := "sh";      /* rename process */
Is there already a worm? /* faults here causes mass infection */
Initialize clock;
while (true) {
    cracksome(); /* attack accounts, try to find hosts */
    sleep(30); /* hide the worm */
    Listen for other worms /* faults here causes mass infection */
    create a new process, kill the old /* Camouflage */
    try to attack some machines;
    sleep(120); /* hide the worm */
    if (running > 12 hours)
        cleaning host List; /* reduce memory consumption */
    if (pleasequit && wordcheck > 10)
        exit
}
```



# Internet Wurm: Lessons Learned

## ■ Verursacher und rechtliche Folgen

- ❑ Robert T. Morris, 23, Cornell Student (Sohn des NSA Chief Scientist)
- ❑ Suspendierung von der Cornell University
- ❑ Verurteilt zu \$ 10.000 und 400 Stunden gemeinnütziger Arbeit

## ■ Lessons Learned

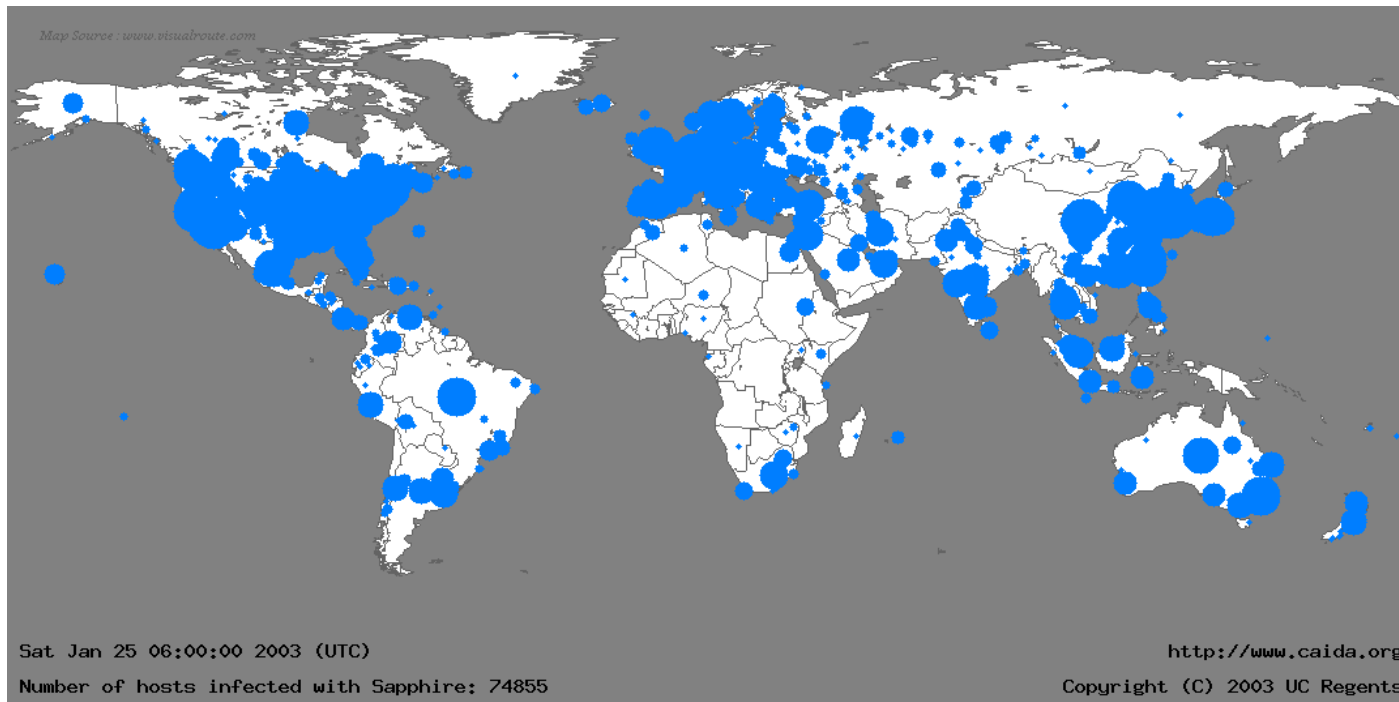
- ❑ (lange) bekannte Bugs fixen
- ❑ Starke Passwörter benutzen
- ❑ Least privilege Prinzip (sowenig Rechte wie nötig), strenge Zugriffskontrolle
- ❑ Logging und Auditing
- ❑ Keine reflexartigen Reaktionen
- ❑ Kontinuierliche Information von sich und anderen
- ❑ „Zentrales“ Security Repository
  - CERT (Computer Emergency Response Team) wurde gegründet  
[www.cert.org](http://www.cert.org)



# Historischer Rückblick II: 2003 Slammer Wurm

## ■ Chronologie

- ❑ Samstag, 25. Januar 2003: Kurz vor 5:30 Uhr (UTC), d.h. 6:30 Uhr (MEZ) taucht der Wurm auf
- ❑ Verbreitung des Wurm um 6:00 Uhr (UTC):

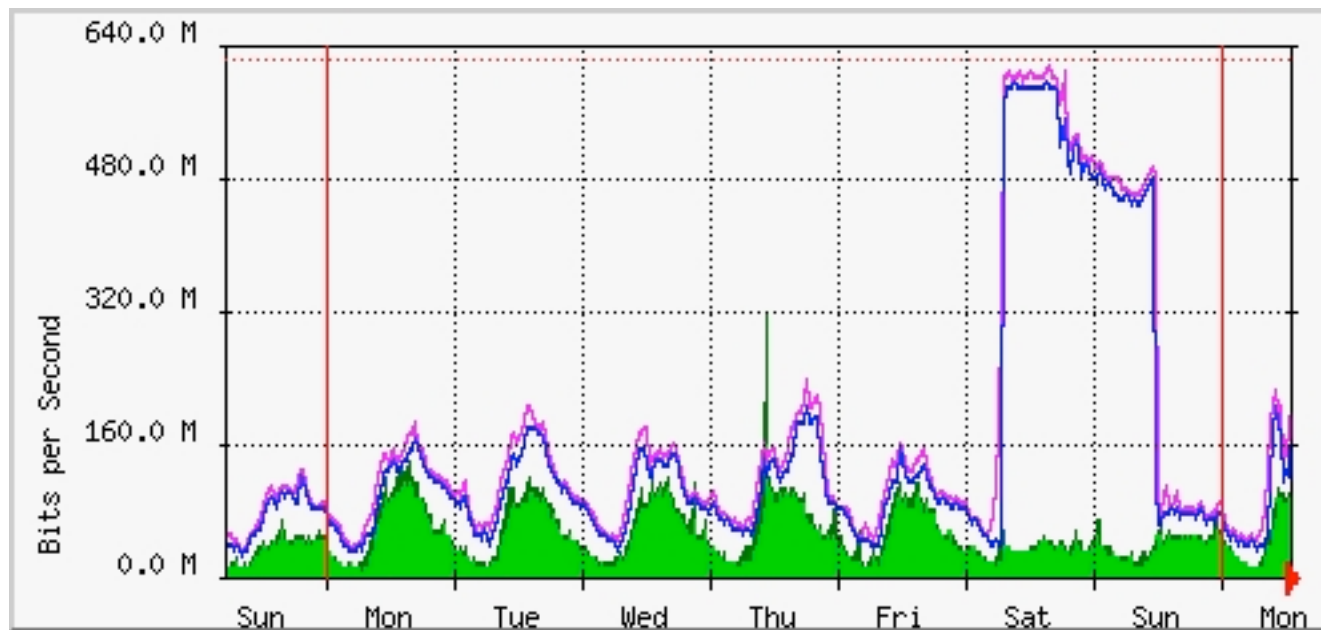


Quelle:  
MPSS 03

Kreisdurchmesser entspricht Anzahl infizierter Hosts (logarithmische Darstellung)

# SQL Slammer im Münchner Wissenschaftsnetz

- Münchner Wissenschaftsnetz (MWN), verbindet u.a. alle Standorte der Münchner Universitäten, der FH und der Bayerischen Akademie der Wissenschaften:  
Massive Störungen von Samstag 25.01.03 6:30 Uhr bis 26.01.03 11:30 Uhr
- Verkehrsstatistik am zentralen Router des MWN (1 Woche)



- Legende
  - Grün: eingehender Verkehr
  - Blau: ausgehender Verkehr
  - Dunkelgrün: Max. Peak im 5 Minuten Intervall (eingehend)
  - Magenta: Max. Peak im 5 Minuten Intervall (ausgehend)

# Slammer Verbreitung und Folgen

## ■ Schnellster Wurm in der Geschichte

- ❑ 1. Minute: Verdopplung der Population alle 8,5 Sekunden ( $\pm 1$  s)
- ❑ > 3 Minuten: etwas verringerte Verbreitungsrate; Netzbandbreite wird zum beschränkenden Faktor
- ❑ 10 Minuten: ca. 90 % aller anfälligen Hosts sind infiziert

## ■ Folgen:

- ❑ Große Teile des Internets nicht mehr erreichbar
- ❑ Steuerungssysteme für die Stromversorgung gestört
- ❑ Funktionsstörungen bei Geldautomaten
- ❑ Steuerrechner von zwei Atomkraftwerken in den USA betroffen
- ❑ .....

# Slammer: Voraussetzungen

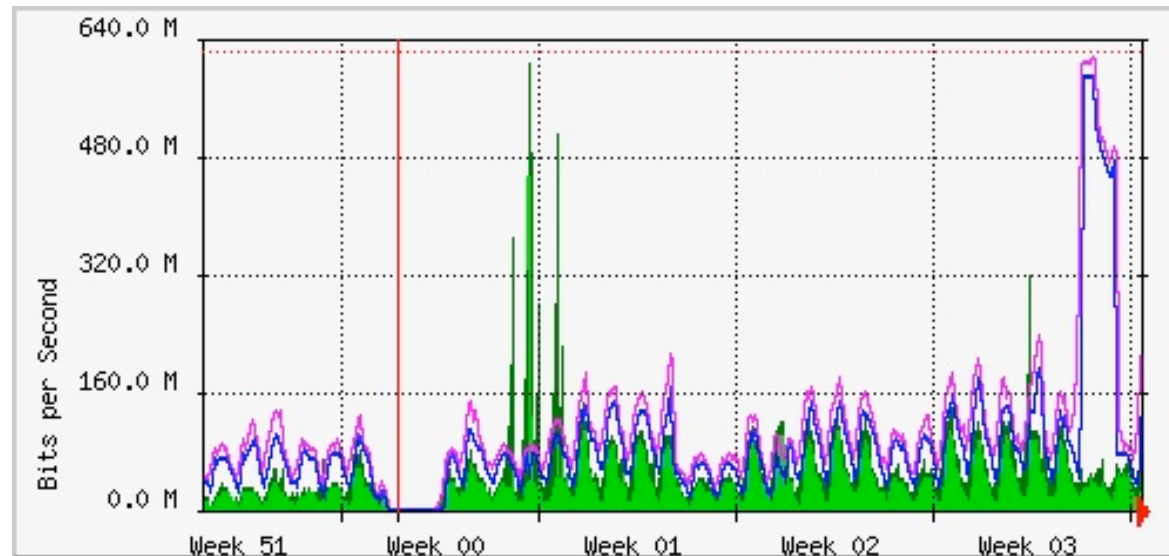
- SQL Server; Client Verbindungen über
  - NetBios (TCP Port 139/445)
  - Sockets (TCP Port 1433)
  - Monitor Port (UDP 1434) zur Ermittlung der Verbindungsart; Client schickt 0x02 an den Port; Server schickt Verbindungsinformationen
- Buffer Overflow Bug im SQL Server
  - Client setzt erstes Bit auf 0x04  
im Bsp. `\x04\x41\x41\x41\x41` (`\x41 = „A“`)
  - SQL Monitor nimmt Rest der Daten und öffnet damit Registry  
`HKLM\Software\Microsoft\Microsoft SQL Server\AAAA`  
`\MSSQLServer\CurrentVersion`
  - Über geeignet formatierte Daten kann hier ein Buffer Overflow herbeigeführt werden
- Problem:
  - SW von Drittanbietern beinhaltet SQL-Server
  - Dies ist nicht allgemein bekannt

# Slammer: How it works

- Slammer passt in ein UDP Packet
  - 376 Byte groß, geschrieben in Assembler
  - Mit Header Informationen 404 Byte
- Slammer nutzt Buffer-Overflow an UDP Port 1434
- Nach Infektion:
  - „Raten“ zufälliger IP-Adressen
  - Angriff über UDP
- Keine Schadfunktionalität im eigentlichen Sinn
- Charakteristika:
  - UDP verbindungsloses Protokoll; wird nur durch Bandbreite beschränkt
  - Höchste beobachtete „Probing“-Rate: 26.000 Scans pro Sekunde
  - Aggressive Verbreitungsstrategie führt dazu, dass der Wurm mit anderen Würmern um Netzbandbreite konkurriert

# Slammer im MWN (Forts.)

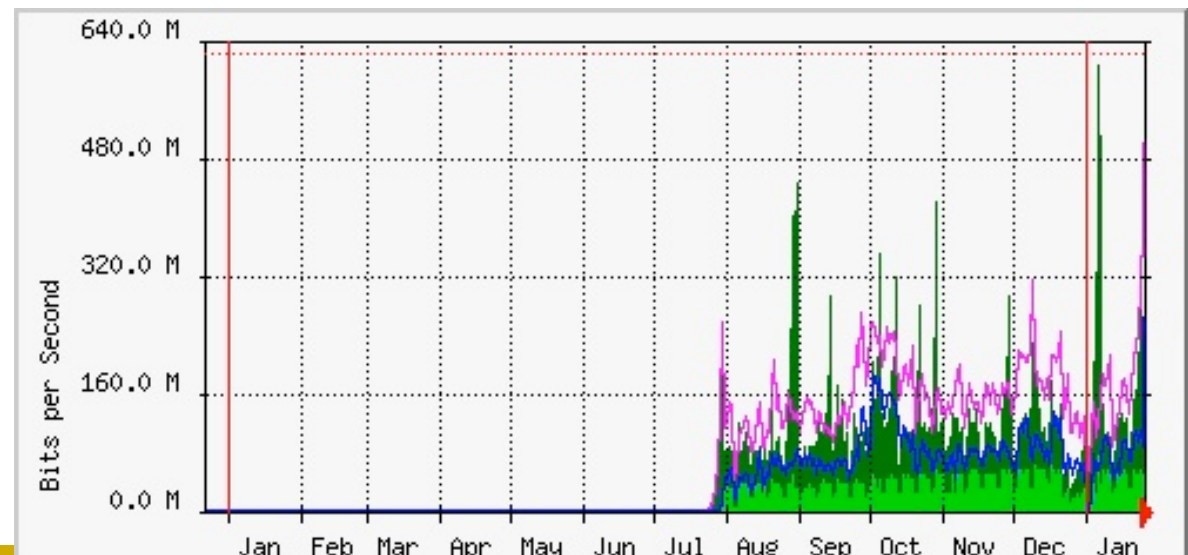
## ■ Monatsstatistik



## ■ Mind. 8 SQL-Server betroffen

## ■ Maßnahmen:

- Zugang zum MWN für diese Server gesperrt
- Port 1434 gesperrt



# Slammer: Lessons Learned

- Grundproblematik:  
Nicht behobenen Bugs in Anwendungen (kein Einspielen von Patches)
- Bundling von Software; Anwender weiß u.U. nichts von Sicherheitsproblemen und notwendigen Patches
- Angriffe über UDP können zu extrem schneller Verbreitung führen
- Gegenmaßnahmen:
  - Filtern des entsprechenden Verkehrs (UDP Port 1434) über Firewall
  - Fehler und Schwächen beheben
  - Nicht notwendige Dienste abschalten

# Vergleich Internet Worm und ILOVEYOU

	<b>Internet Worm</b>	<b>Slammer</b>
Angegriffene Hosts/OS	SUN und VAX / UNIX	Microsoft Windows/SQL Server
Angriffsstrategie	Ziemlich komplex Nutzt eine Vielzahl von Bugs und fortschrittliche Strategien	Einfaches Assembler Programm nutzt Buffer Overflow
Schadfunktion	Verursacht große Load und viel Netzverkehr	Verursacht extremste Load und Netzverkehr
Verbreitung	~ 6.000 Systeme Ziemlich schnell	Extrem schnell 90 % aller verwundbaren Systeme nach 10 Minuten infiziert



# Stuxnet: Presse-Echo

- ❑ New spy rootkit targets industrial secrets - Windows virus takes aim at Siemens SCADA management systems (techworld.com, 19.07.10)
- ❑ Trojaner per USB-Stick - Siemens und der digitale Industrie-Spion (Sueddeutsche.de, 21.07.10)
- ❑ Stuxnet-Wurm kann Industrieanlagen steuern (heise.de, 16.09.10)
- ❑ Computervirus Stuxnet - Der Wurm, der aus dem Nichts kam (Spiegel Online 22.09.10)
- ❑ Der digitale Erstschlag ist erfolgt (FAZ, 22.09.10)
- ❑ A Silent Attack, but Not a Subtle One (New York Times, 26.09.10)
- ❑ Computervirus Stuxnet traf auch deutsch Industrie (Sueddetusche.de, 02.10.10)
- ❑ Stuxnet breitet sich weiter aus (Financial Times Deutschland, 4.10.10)
- ❑ Stuxnet: Vorgeschmack auf den Cyber-Krieg? (Deutsche Welle, 5.10.10)
- ❑ ....

# Stuxnet

- Befällt Windows-Rechner (z.T. über Zero-Day-Exploits)
  - autorun.inf-Dateien können von Windows auch als EXE-Datei interpretiert werden
  - Windows Server Service RPC Handling vulnerability, aka. Conficker Bug (CVE-2008-4250, bekannt seit 25.09.08, Patch 26.10.08)
  - LNK / CLINK: LNK-Datei auf USB Stick; Beim Lesen des Icons einer LNK-Datei wird Code ausgeführt (CVE-2010-2568, bekannt seit 30.06., Patch 2.08.)
  - Payload-Dateien; Treiber (MrxCls.sys, MrxNet.sys) sind digital signiert mit Zertifikaten von Realtek bzw. JMicron
    - Treiber stellen Verbreitung auch nach Neustart sicher
  - Print Spooler Bug: Fehler in Druckerwarteschlange erlaubt Schreiben in Systemverzeichnis (CVE-2010-2729 bekannt seit 14.07., Patch 14.09.)
  - Privilege escalation über Keyboard layout file (Patch 12.10.)
  - Privilege escalation über Task Scheduler (Patch 14.12.10)

# Stuxnet

## ■ Infektion des Windows-Rechner

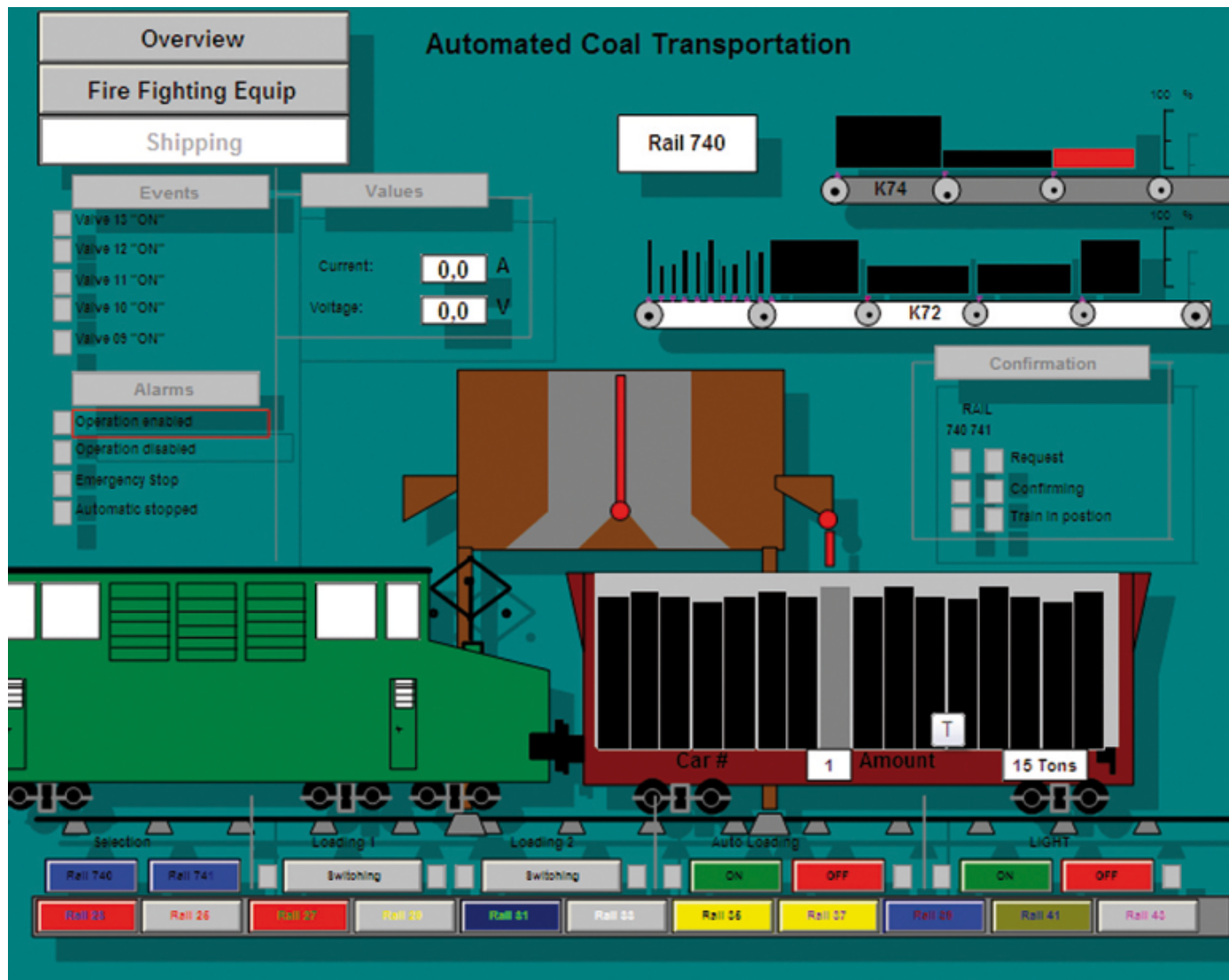
- ❑ Versucht sich über LAN zu verbreiten, in dem nur eingeschränkte oder keine Internet-Konnektivität besteht
- ❑ Installation von RPC-Server und Client
- ❑ Peer-to-Peer Kommunikation zwischen infizierten Rechnern
- ❑ Damit Update-Möglichkeit für neuere Versionen
- ❑ Versuch Datei-Freigaben für Weiterverbreitung zu nutzen
- ❑ Installation eines Windows-Rootkit

## ■ eigentliches Ziel: WinCC Software zum Management speicherprogrammierbarer Steuerungen (SPS) (engl. SCADA [supervisory control and data acquisition]) von Industrieanlagen

# Siemens SCADA System SIMATIC WinCC

- „Process visualization with Plant Intelligence“
- Universell einsetzbare Software zur Steuerung und Automatisierung von Industrieanlagen:
  - Automobilproduktion und Zulieferindustrie
  - Chemische und pharmazeutische Industrie
  - Ernährungs-, Getränke- und Tabakindustrie
  - Maschinenbau
  - Energieerzeugung und Verteilung
  - Handel- und Dienstleistungsgewerbe
  - Kunststoffverarbeitende Industrie
  - Metallverarbeitende Industrie und Stahlindustrie
  - Papierverarbeitung und Druckindustrie
  - Verkehr, Transportgewerbe und Logistik
  - Wasserversorgung und Müllentsorgung

# Bsp.: Prozessabbild für Kohlentransport



Quelle: [www.automation.siemens.com](http://www.automation.siemens.com)



# Angriff auf WinCC bzw. SCADA

- Infizierter Windows Rechner
- Suche nach WinCC oder Siemens Step7 Software in Registry
- Verbindung zum WinCC Datenbank-Server mit
  - fest-kodiertem Account und Passwort
  - uid= WinCCConnec    pwd= 2WSXcder
- Siemens empfiehlt, wegen Stabilität der Steuerung, diesen Account nicht zu verändern
- Malicious SQL-Statement
  - Transfer von Stuxnet-Code auf Rechner mit WinCC
  - Stuxnet schreibt sich in Step7 Datenbank
  - Modifikation von WinCC Views führen zur Ausführung von Schadcode

# Eigentliches Ziel von Stuxnet

- Infektion von programmable logic device contollern (PLCs)
- Ersatz einer zentralen DLL (s7otbxdx.dll), damit:
  - Monitoring aller Lese- und Schreibzugriffe auf PLC
  - Infektion eines PLC mit eigenen Code Blöcken
  - Masquerading einer PLC Infektion (PLC-Rootkit)
- Infizierter PLC arbeitet auch ohne Verbindung zum Steuerrechner „weiter“



# Angriff auf PLC

- Drei Stuxnet-Varianten (A,B,C) abhängig von verwendeter CPU
- Funktionsweise von A und B konnte geklärt werden:
  - Infektion erfolgt wenn Programm-Baustein FC1869 definiert und ein bestimmtes Kommunikationsmodul (CP-342-5) registriert sind
  - Kommunikationsmodule (bis zu 6) steuern je 31 Frequenzumformer, die Drehgeschwindigkeit von Elektromotoren steuern
  - Endlicher Automat in Stuxnet verändert in unregelmäßigem Abstand (13 Tage bis 3 Monate) die Frequenz
  - Variante A für Frequenzumformer der Firma Vacon (Finnland)
  - Variante B für Umformer der Fa. Fararo Paya (Teheran)
- C deaktiviert oder nur teilweise fertig

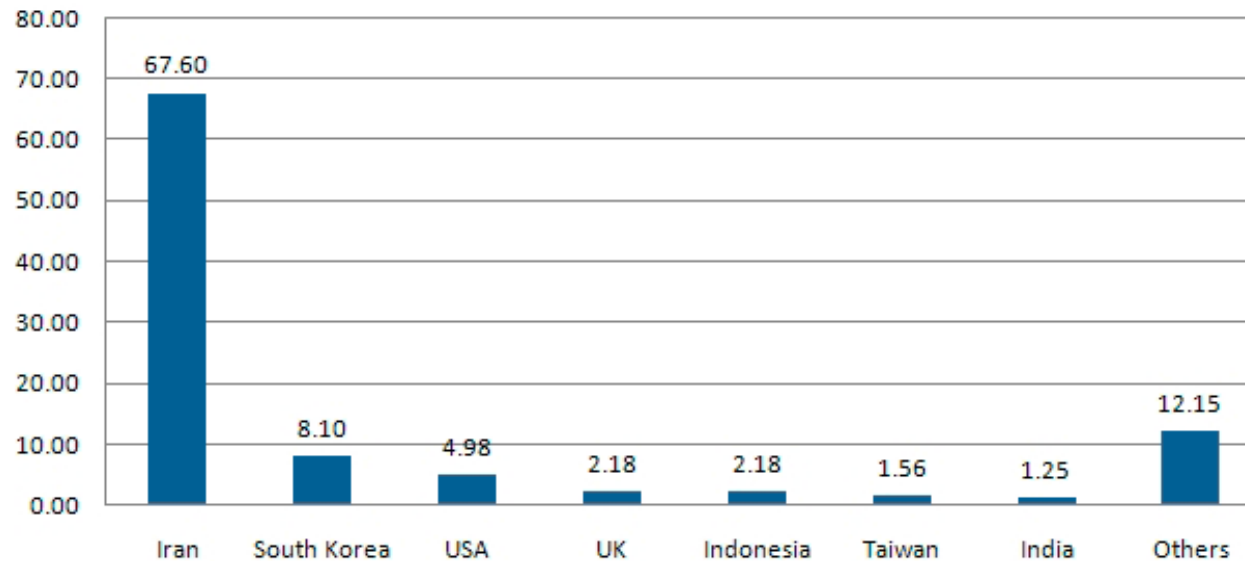
# Stuxnet: Verbreitung

- Infektion von Wechselmedien
- Kopiert sich selbst in Siemens Step7 Projekte
  - Ausführung des Schad-Codes beim Öffnen des Projekts
- Verbreitung über das Netz:
  - Infizierte Systeme bilden Peer-to-Peer Netz z.B. für Updates
  - Infektion von WinCC Maschinen über „Well-Know“ Datenbank Passwort
  - Weiterverbreitung über Windows Netz-Shares
  - Weiterverbreitung über Wechselmedien (z.B. USB-Sticks)
  - Verbreitung über Print Spooler Bug
  - Windows Server Service RPC Vulnerability
- Verbreitung auf PCs sehr viel größer als auf Anlagensteuerungen (Baustein FC1896 erforderlich)

# Stuxnet: lokale Verbreitung

## ■ Symantec: w32\_stuxnet\_dossier.pdf

Percentage of Stuxnet infected Hosts with Siemens Software installed



## ■ [www.eset.com](http://www.eset.com): Stuxnet\_UNDER-theMicroscope.pdf

Table 1.4.1 – The Percentage Distribution of Infections by Region

Iran	Indonesia	India	Pakistan	Uzbekistan	Russia	Kazakhstan	Belarus
52,2%	17,4%	11,3%	3,6%	2,6%	2,1%	1,3%	1,1%
Kyrgyzstan	Azerbaijan	United States	Cuba	Tajikistan	Afghanistan	Rest of the world	
1,0%	0,7%	0,6%	0,6%	0,5%	0,3%	4,6%	

# Stuxnet - Analyse

- Viele verschiedene Exploits um Hostrechner anzugreifen
- Mehrere Zero-Day Vulnerabilities
- „Maskierung als Treiber mit „legaler“ Signatur
- Verschlüsselte Konfigurationen
- „Infektion“ von Dynamischen Bibliotheken (dll)
  - Systembibliotheken (Nt.sys.dll)
  - ca. 10 Anti-Viren Programme (Kaspersky, McAfee, F-Secure,....)
- Komplexer Angriffs- und Installationsvektor
- Installation einer Backdoor; Command and Control Server:
  - [www.mypremierfutbol.com](http://www.mypremierfutbol.com)
  - [www.tudaysfutbol.com](http://www.tudaysfutbol.com)
- Funktion eines Windows Rootkits
- Injektion von Code in PLC Systeme
- Masquerading der Infektion auch auch PLCs (PLC-Rootkit)

# Stuxnet - Analyse

- Ungewöhnlich grosses Binary für einen Wurm
- Extrem grosse Komplexität
- „Only few attackers will be capable of producing a similar attack“
- Damit Angriffe auf „kritische Infrastrukturen“ möglich
- „We conducted a detailed technical analysis of the worm Win32/Stuxnet, which currently is perhaps the most technologically sophisticated malicious program developed for a targeted attack to date.“ (eset)
- „Stuxnet is the type of threat we hope to never see again.“(Symantec)

# Vermutungen über Verursacher und Ziele

- Experten vermuten größten Aufwand und teuerste Entwicklung von Malware in der Geschichte
- Fachleute aus unterschiedlichen Bereichen notwendig
- Nicht bestätigte/belegte Vermutungen:
  - Israelischer Geheimdienst mit Unterstützung der USA
- Vermutete Ziele:
  - Atomkraftwerk Bushehr im Iran
  - Iranische Urananreicherungsanlage in Natanz
    - Manipulation der Geschwindigkeit der Zentrifugen:
    - Normalwert 1064 Hz
    - Stuxnet erhöht die Frequenz für 15 Min. auf 1.410 Hz
    - Nach 27 Tagen Reduzierung auf wenige hundert Herz
    - Folge: Zerstörung der Zentrifugen
    - Wiki-Leaks meldet nuklearen Störfall in Natanz (17.07.2009)
    - Von 4.700 Zentrifugen arbeiten zu der Zeit nur 3.900

# Einschub: Bundestrojaner

- Chaos Computer Club (CCC) analysiert ihnen zugespielte DLL: mfc42u1.dll
- Veröffentlicht Analyse (8.10.11) (<http://www.ccc.de/system/uploads/76/original/staatstrojaner-report23.pdf>)
- Funktionen
  - Screenshots
  - Abhören von Skype und VoIP Gesprächen
  - Nachladen weiterer Module
  - Kommunikation mit Command and Control (C&C) Server in **Ohio USA**
- **Erhebliche** Implementierungsfehler (genaue Analyse in Kap. 3)
  - Keine Authentisierung (Kap. 8)
  - Verschlüsselungsmodus (AES-ECB) ungenügend (Kap. 4 und 5)
- Dadurch: Übernahme des Trojaners durch Dritte möglich

# Einschub: Bundestrojaner - Rechtliche Aspekte

- Zunehmend verschlüsselte Kommunikation
- Ermittlungsbehörden reagieren mit Quellen-Telekommunikationsüberwachung (TKÜ) basierend auf §100a StPO
- TKÜ: Abhören von Telefon (nicht nur klassisch)
- Stichwort: Online-Durchsuchung
- Strenge Einschränkung durch Urteil des Bundesverfassungsgericht 2008:
  - Gefahr für: Leib, Leben, Freiheit einer Person, Bestand des Staates,
- Landshuter Anwalt übergibt Trojaner an CCC
  - Ermittlung wegen Drogendelikten
  - Anwalt findet Screenshots vom Computer des Mandanten
  - Landgericht Landshut erklärt diese Maßnahme (begründet mit Quellen-TKÜ) für rechtswiedrig (Januar 2011)