Stuxnet – The first Cyberweapon?

von Andreas Benzin

Inhalt

1. Überblick / Angriffsszenario
2. Malware-Dropper
   - Reproduktionsmethoden
   - Installation
3. Payload
   - SPS-Rootkit
   - Infektion der SPS
   - Funktionsweise der Schadprogramme
   - Hinweise auf Urananreicherungsanlage in Natanz
4. Zusammenfassung

Überblick *Angriffsszenario*

von allen Netzwerken isolierte Umgebung

Internet

Firmen-LAN

Wechsel-datenträger

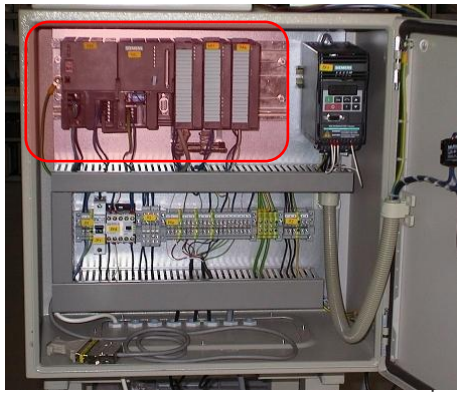
Entwicklungs-PC (Windows)

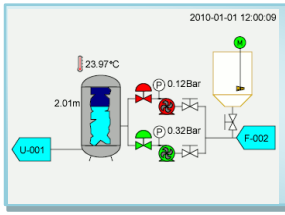
Siemens Step 7 IDE

USB-Stick

Programmier-PC (Windows)
(z.B. Siemens „Field-PG“)

Step 7





Prozessvi-sualisierung (WinCC)

virtuelle Welt

reale Welt

Siemens Simatic SPS

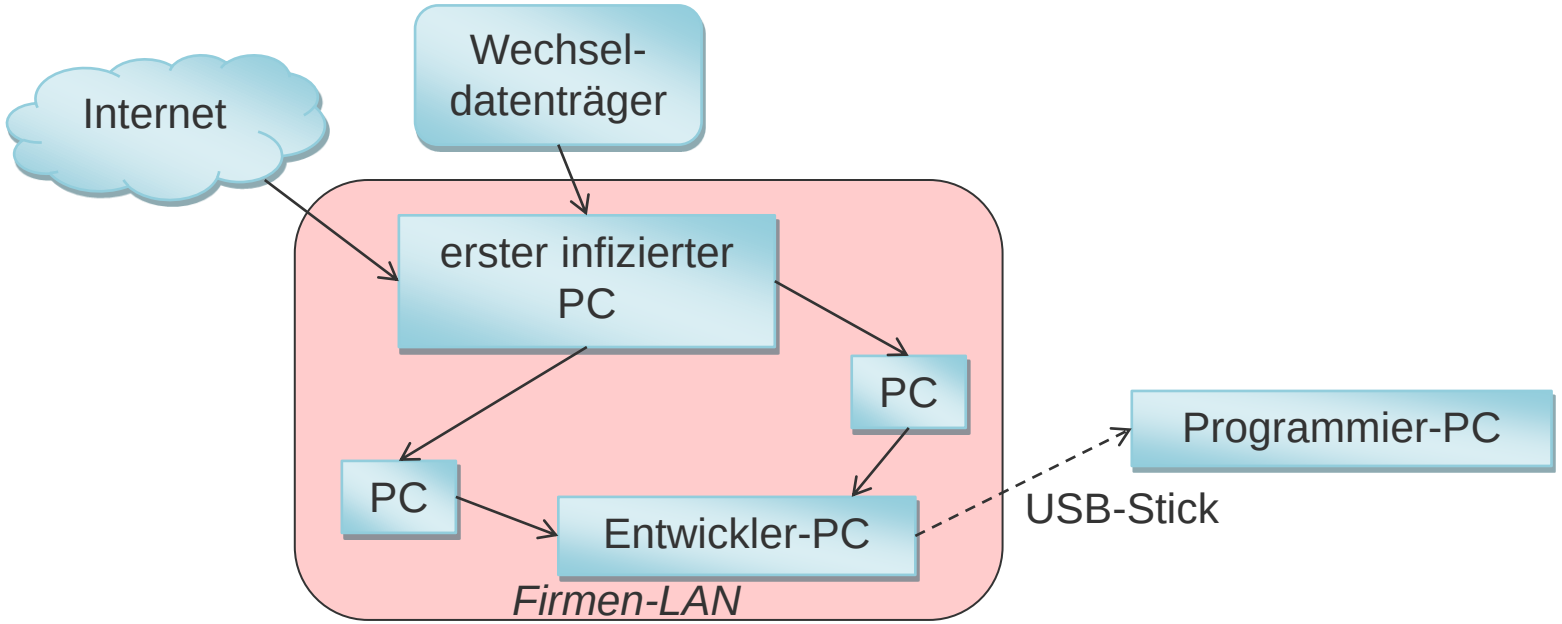
Sensoren
(z.B. Temperatur, Druck, Füllstand)

Aktoren
(z.B. Motoren, Pumpen, Ventile)

Malware-Dropper *Reproduktionsmethoden (Wurm-Funktionalität)*

Computernetzwerke

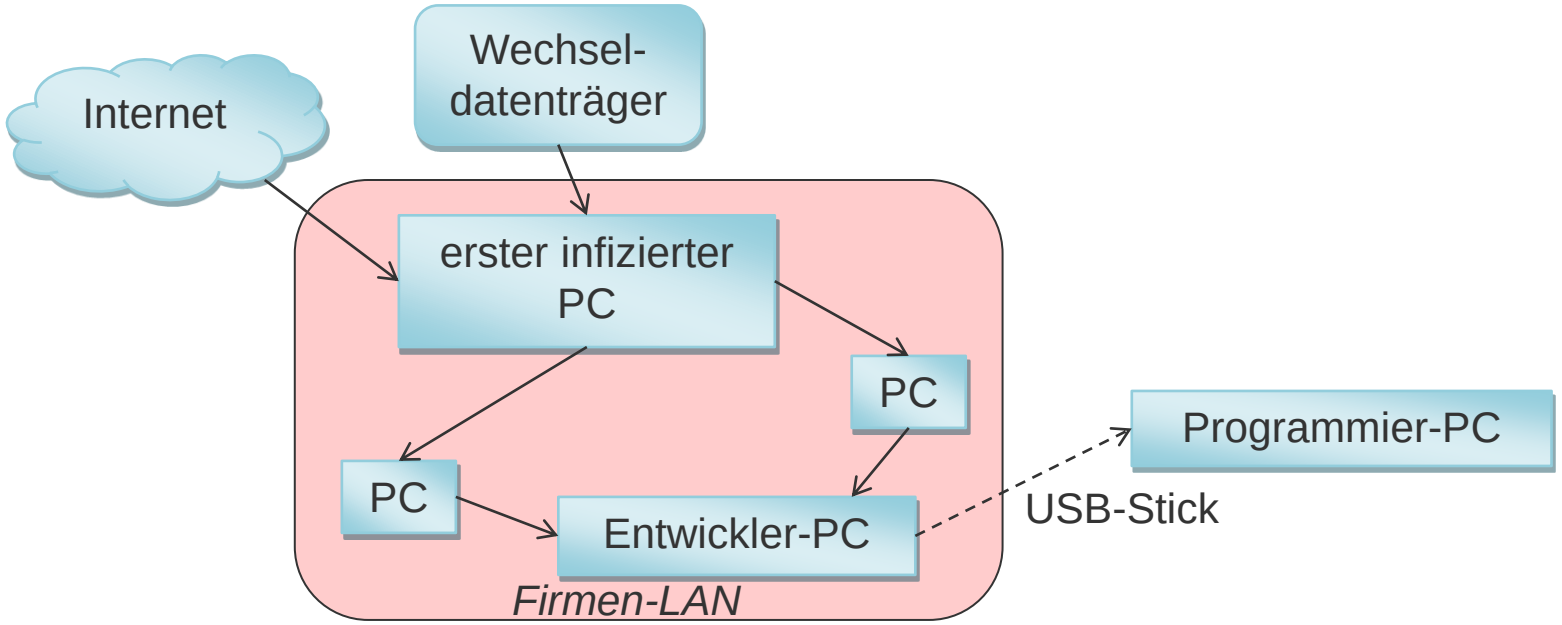
- Microsoft Dateifreigaben (RCE über WMI Instruktionen)
- Microsoft Druckerfreigaben (*Zero-Day:* „Printer Spooler Vulnerability“)
- Windows Server Service (Exploit in SMB-Protokoll, RCE über RPC-Request)
- Siemens WinCC SQL-Datenbank (*Zero-Day:* hartcodiertes Passwort)
- verteilte P2P-Updates (über RPC-Server/Client)



Malware-Dropper *Reproduktionsmethoden (Wurm-Funktionalität)*

Wechseldatenträger

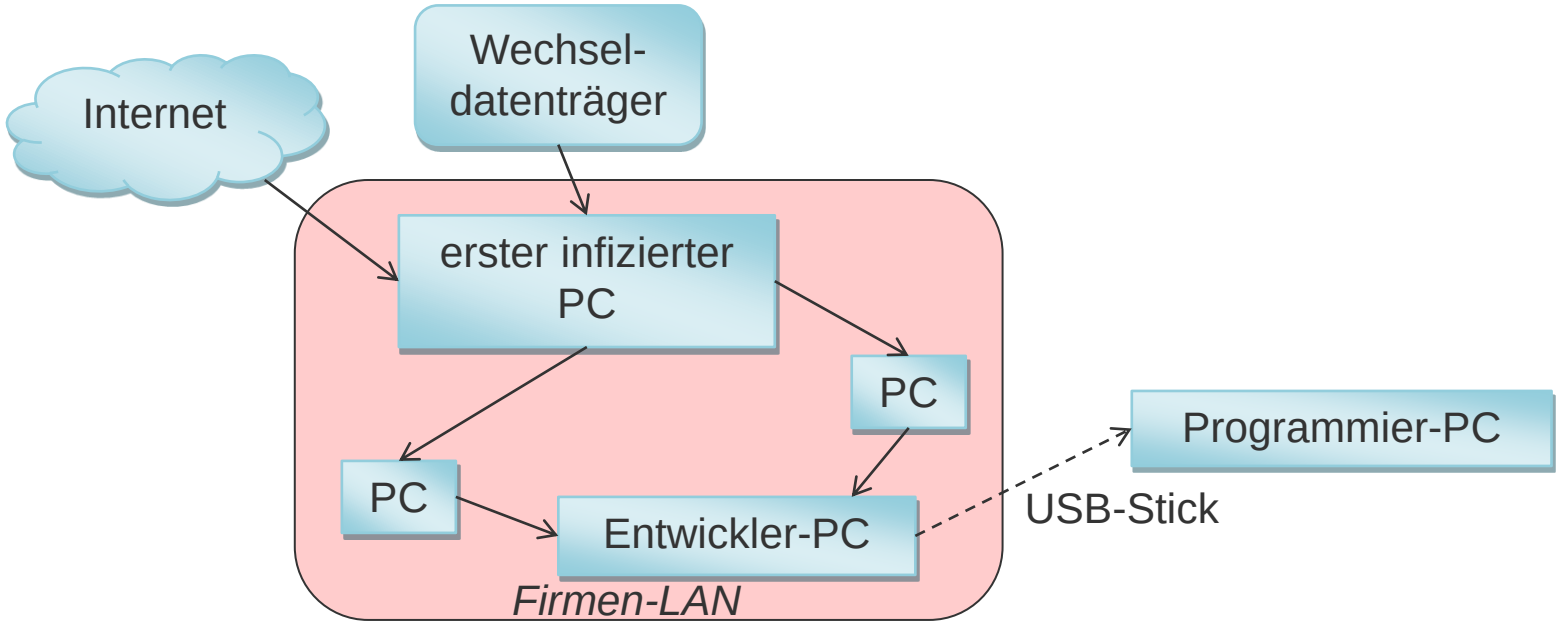
- Permanente Überwachung der Laufwerke
- Rootkit zum Verbergen des Stuxnet-Droppers
- Code-Execution über *Zero-Day:* „LNK-Vulnerability“ (extrem mächtig)
- Quick & Dirty Rootkit nach Ausführung
- Erstinfektion vermutlich über USB-Stick



Malware-Dropper *Reproduktionsmethoden (Wurm-Funktionalität)*

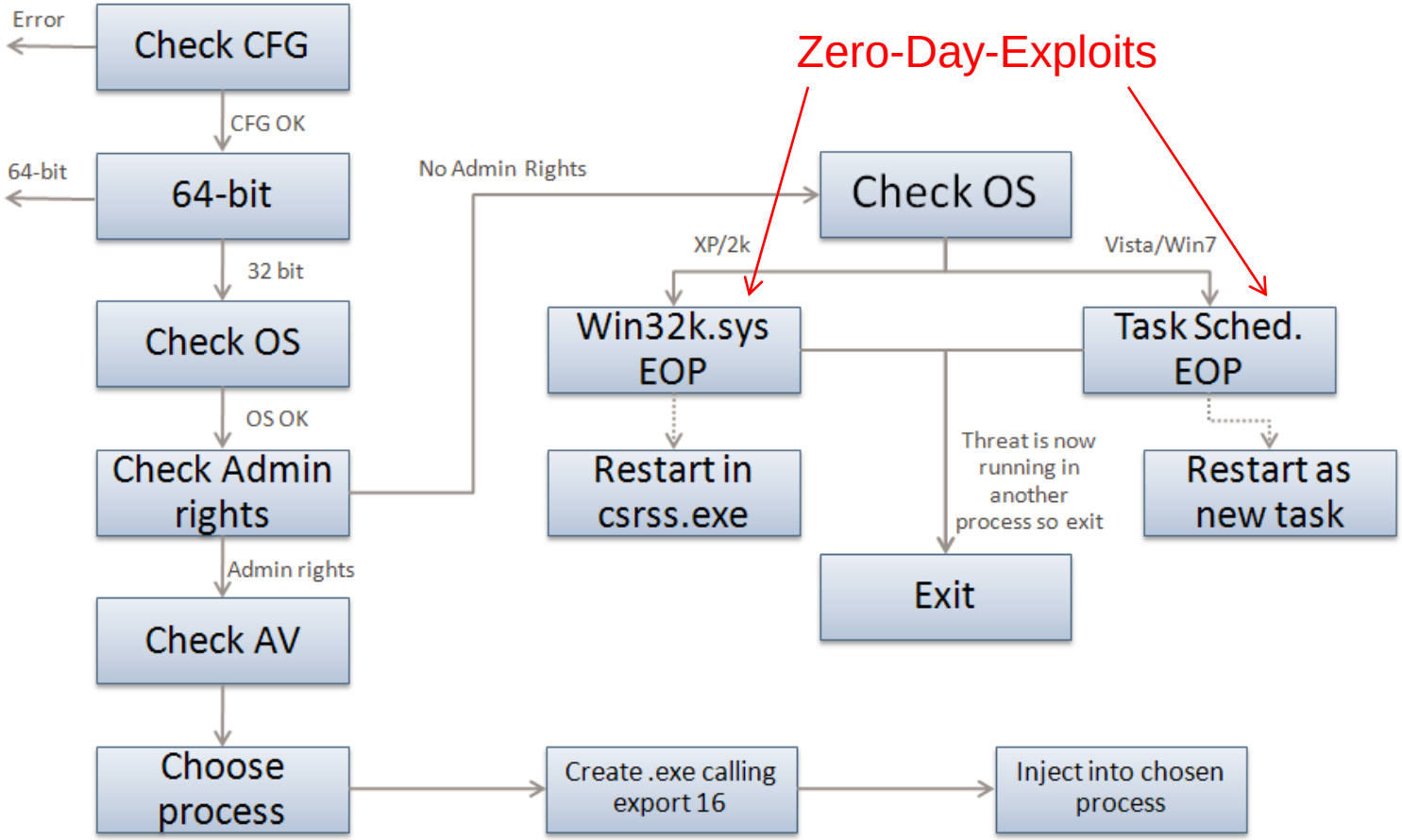
Siemens Step7 Projektdateien

- Infizierung von allen Step7-Projektdateien mit Stuxnet-Dropper und Starter
- Virus-Funktionalität



Malware-Dropper *Installation*

Das Erlangen von Admin-Rechten:



z.B. lsass.exe / winlogon.exe / svchost.exe

Hauptinstallationsroutine wird in Prozess injiziert

Malware-Dropper *Installation*

Hauptinstallation (immer über Code-Injektion in Systemprozesse):

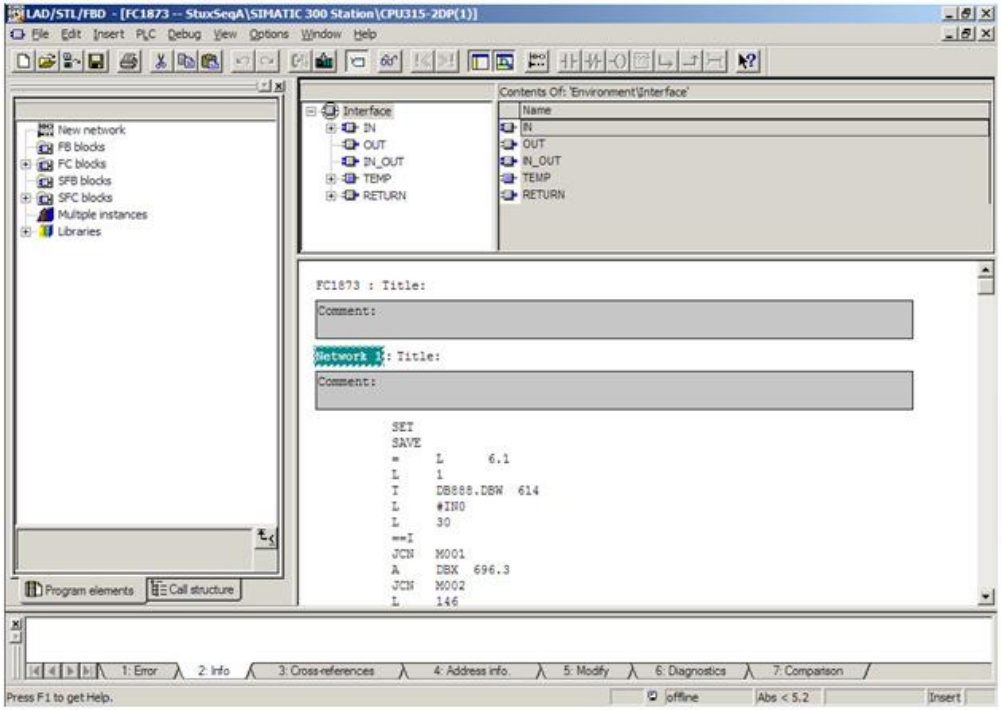
- Replizierungsmethoden (z.B. RPC-Server/Client, Wechseldatenträger-Deamon, usw.)
- Windows Rootkit
- manipulierte Step7 „s7otbxdx.dll“ (Payload)

Windows-Rootkit:

- zwei Treiber werden mit gestohlenen digitalen Zertifikaten von Realtek oder JMicron installiert (werden bei Windows-Boot früh geladen)
- **Persistenz und Ausführung**: „mrxcls.sys“ (injiziert Stuxnet-Code in System- und Step7-Prozesse)
- **Verschleierung**: „mrxnet.sys“ (fängt I/O-Request-Packets an Kernel ab und löscht Stuxnet-Dropper-Files aus Kernel-Antworten heraus)
- Command & Control Server mit Backdoor-Funktionalität über HTTP (Ausführung über Code-Inkjektion in Internet-Explorer Prozess)

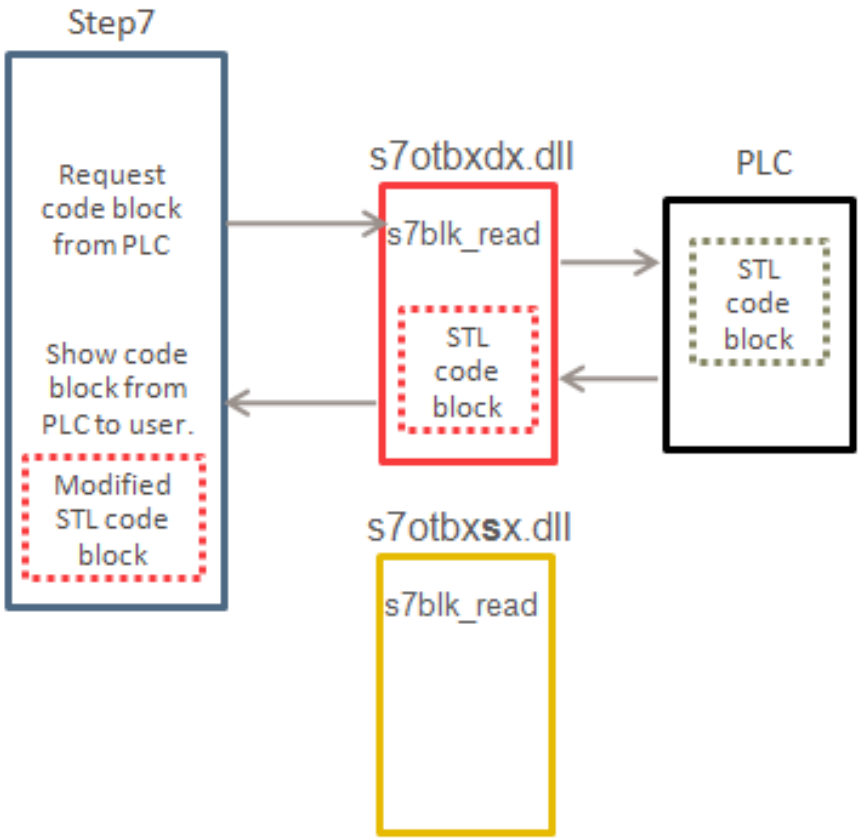
Payload *Überblick*

- Step7 Treiber „s7otbxds.dll“ wird ersetzt
- „s7otbxds.dll“ bietet Funktionen an, um z.B. Daten von einer angeschlossenen SPS zu lesen oder zu schreiben
- Stuxnet hat so volle Kontrolle über I/O-Verkehr zur SPS
- **Rootkit-Funktionalität und Infektion der SPS mit der Schadroutine wird realisiert**



Payload *SPS-Rootkit*

- Read-Requests werden abgefangen und Stuxnet-Code auf der SPS für den Benutzer verschleiert



Payload *Infektion der SPS*

Stuxnet liest den „System Data Block“ einer SPS aus und befällt nur bestimmte Konfigurationen:

- SPS-Typ: Siemens S7-315-2 & Siemens S7-417
- bei S7-315-2: Zusatzmodul CP342-5 (zusätzliche Profibus-Kommunikation)
- bei S7-315-2: mindestens 33 Frequenzumrichter von Vacon oder Fararo Paya an Profibus angeschlossen
- bei S7-417: nicht vollständig bekannt

Stuxnet-Entwickler müssen ausführliche Kenntnisse über Anlagenkonfiguration gehabt haben. Verhinderung von Kollateralschäden.

Payload *Funktionsweise des S7-315-2 Sabotageprogramms*

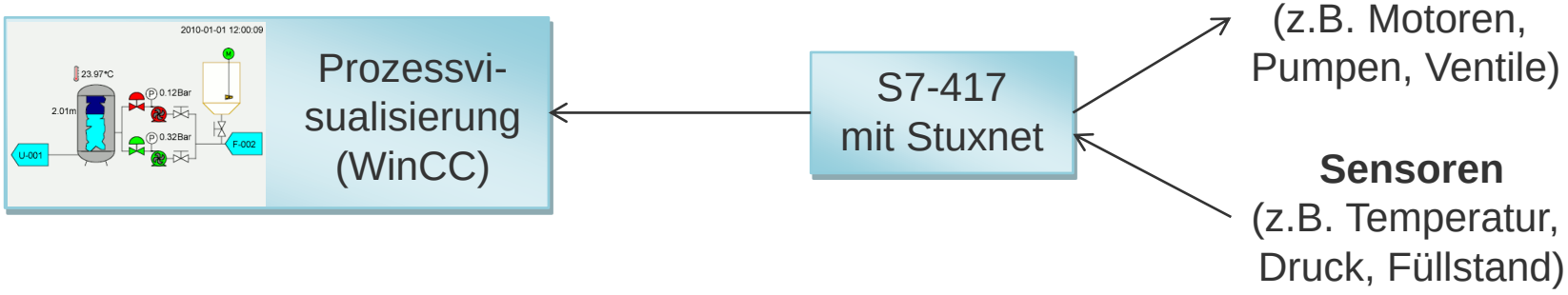
- normales SPS Programm wird nicht überschrieben
- Stuxnet infiziert:
  - Main ISR („OB1“)
  - Watchdog ISR („OB35“)
  - DP_RECV-Funktion (Profibus Kommunikation)

- Zustandsautomat:
  - über längere Zeit Überwachung der Motorfrequenzen (→ 807Hz - 1210Hz)
  - Manipulationsroutine: Drehzahlen von 2Hz – 1410Hz für max. 50 min. variiert
  - Neustart des Zustandsautomaten

- erneuet Überprüfung der Anlagenkonfiguration
- schleichende Zerstörung der Zentrifugen

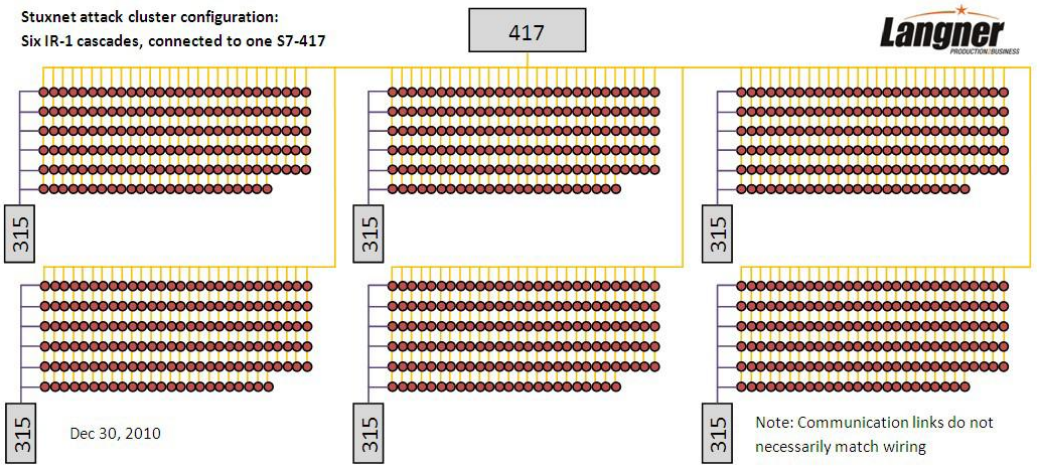
Payload *Funktionsweise des S7-417 Sabotageprogramms*

- Infizierung ähnlich wie bei S7-315-2
- komplexerer Zustandsautomat
- Man-in-the-Middle-Angriff
- Denial-of-Control
- Denial-of-View
- Steuerung von Pumpen & Ventilen
- Überwachung der Betriebsparameter, Sicherheitssystem



Payload *Hinweise auf Urananreicherungsanlage in Natanz*

- S7-417: 6x164 Input-Daten Array → Natanz: 6 Kaskaden mit jeweils 164 Zentrifugen
- S7-315-2: 6 Profibus-Module mit max. 31 Teilnehmern

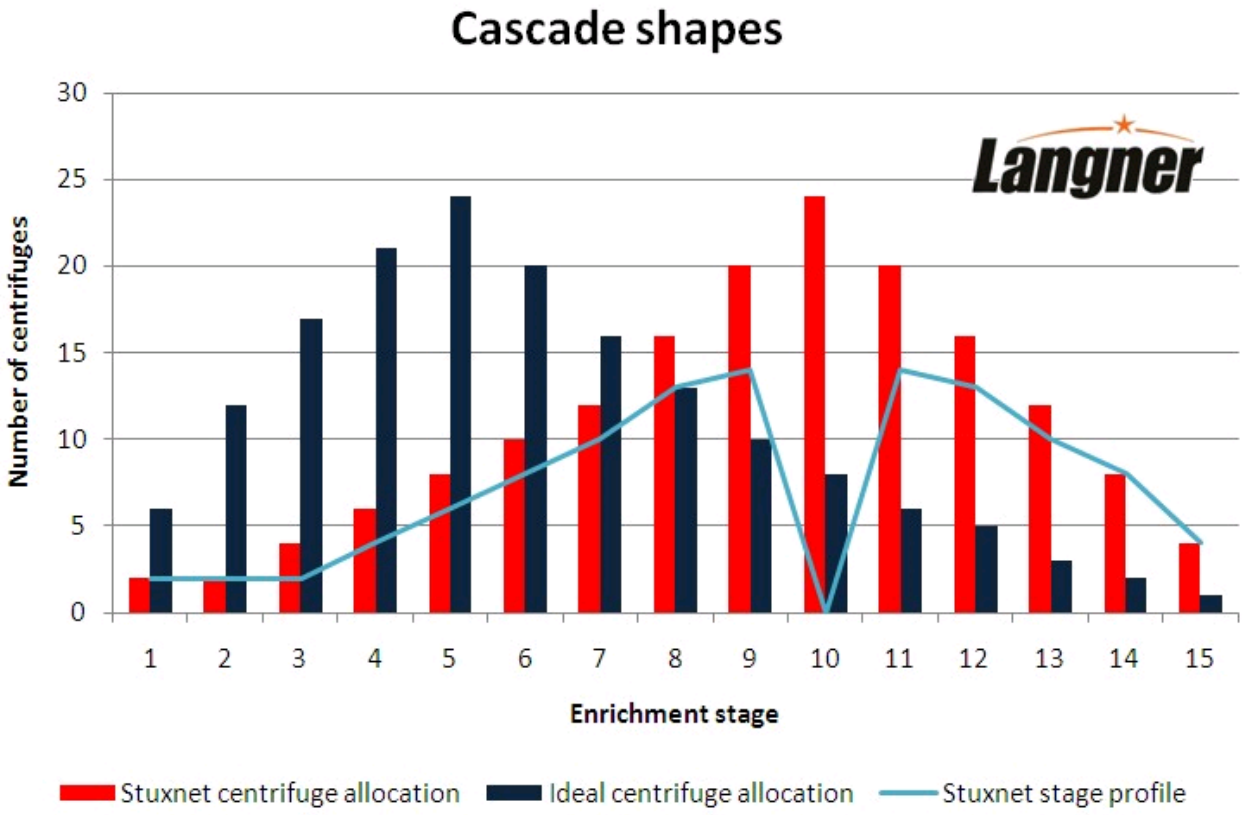


Payload *Hinweise auf Urananreicherungsanlage in Natanz*

- S7-315-2: Nominalfrequenz 1064Hz → Natanz: 1064Hz Rotorgeschwindigkeit
- S7-315-2: Max. Frequenz 1410Hz → Natanz: 1400Hz-1432Hz max.

Payload *Hinweise auf Urananreicherungsanlage in Natanz*

- S7-417: Verteilung des Uranhexafluoridgases auf die Zentrifugen → Ausbeute wird durch Stuxnet extrem vermindert



Payload *Hinweise auf Urananreicherungsanlage in Natanz*

- Iran tauschte Ende 2009 ca. 1000 seiner Uranzentrifugen aus (6x164=984)
- Präsident Mahmoud Ahmadinejad (November 2010):

“They succeeded in creating problems for a limited number of our centrifuges with the software they had installed in electronic parts” (BBC News)

Zusammenfassung *Besonderheiten des Stuxnet-Wurms*

Payload

- erste Schadsoftware, die eine SPS kompromittiert und ein reales physikalisches Industriesystem zerstört hat
- gerichteter (militärischer) Präzisionsangriff auf eine ganz bestimmte Anlagenkonfiguration
- hat evtl. konventionellen Militärschlag ersetzt
- erster Man-in-the-Middle Angriff auf einer SPS
- erstes SPS Rootkit

Malware-Dropper

- 4 Microsoft Windows Zero-Day-Exploits (lauffähig auf *allen* relevanten Windows-Versionen)
- 1 Siemens WinCC Zero-Day-Exploit
- 2 gestohlene digitale Treiberzertifikate

- revolutionärster Wurm in den letzten 20 Jahren; kann als erste echte Cyberweapon bezeichnet werden

Freie Universität Berlin

Danke!

Quellen

Langner, Ralph: *Cracking Stuxnet, a 21st-century cyber weapon.* TED Talks, März 2011

Falliere, Nicolas; O Murchu, Liam; Chien, Eric: *W32.Stuxnet Dossier Version 1.4 (February 2011).* Symantec Corporation, Februar 2011

Albright, David; Brannan, Paul; Walrond, Christina: *Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant? (ISIS Report).* Institute for Science and International Security, 22. Dezember 2010

Langner, Ralph: *How to Hijack a Controller - Why Stuxnet Isn't Just About Siemens' PLCs.* Control Magazine, 13. Januar 2011

Siehe auch http://cst.mi.fu-berlin.de/teaching/SS11/19510b-PS-TI/andreas-benzin-report.pdf für Quellenangaben

Bilderquellen

S. 1: http://www.upi.com/News_Photos/Features/The-Nuclear-Issue-in-Iran/1581/3/#!/1/

S. 1: http://www.servicelab.co.uk/servicelab/servicelab.nsf/id/pa_optimierung.html

S. 3: http://de.wikipedia.org/wiki/Spezial:Linkliste/Datei:Scada_std_anim_no_lang.gif

S. 3: http://de.wikipedia.org/wiki/Spezial:Linkliste/Datei:Mannheim-grosskraftwerk.jpg

S. 7: Falliere, Nicolas; O Murchu, Liam; Chien, Eric: *W32.Stuxnet Dossier Version 1.4 (February 2011)*. S. 16

S. 9: ibid. S. 37

S. 10: ibid. S. 38

S. 12: ibid. S. 39

S. 11: http://www.iet-gmbh.de/ und Siemens

S. 14: http://www.langner.com/en/2010/12/30

S. 15: www.president.ir/piri/media/main/28858.jpg

S. 16: http://www.langner.com/en/2011/01/30/

Alle links vom 20.06.2011