Entwicklung und Analyse eines polymorphen Virus unter Windows 32

Lukas Hermes

Carl von Ossietzky Universität Oldenburg

20. November 2015

Gliederung

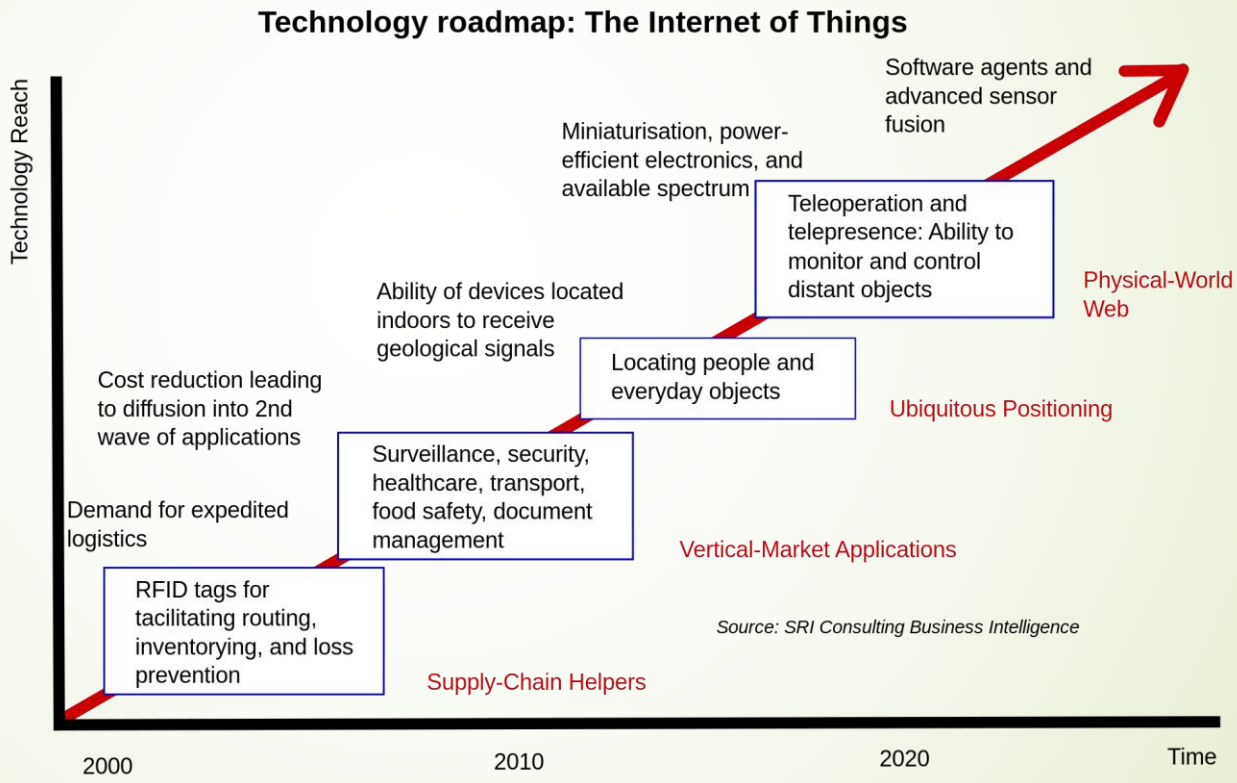
- Motivation
- Der Virus
  - Definition
  - Abgrenzung zu anderer Malware
  - Funktionsweise
  - Wirt
- Die Polymorphic Engine
  - Definition
  - Funktionsweise
  - Zusammenspiel mit dem Virus
- Herangehensweise
  - Literatur
  - Tools
  - Zeitplan
  - Ziele der Bachelorarbeit

Motivation

Fortschreitende Digitalisierung der Gesellschaft

- Industrie 4.0 (Deutschland)
- Industrial Internet Consortium(IIC, Amerika)
  - AT&T, Cisco, General Electric, IBM, Intel
- The Internet of Things(Internet der Dinge)
- Smartphones bzw. Smartwatches

➢ Verschmelzung von physikalischer und digitaler Welt



Quelle: https://en.wikipedia.org/wiki/Internet_of_Things

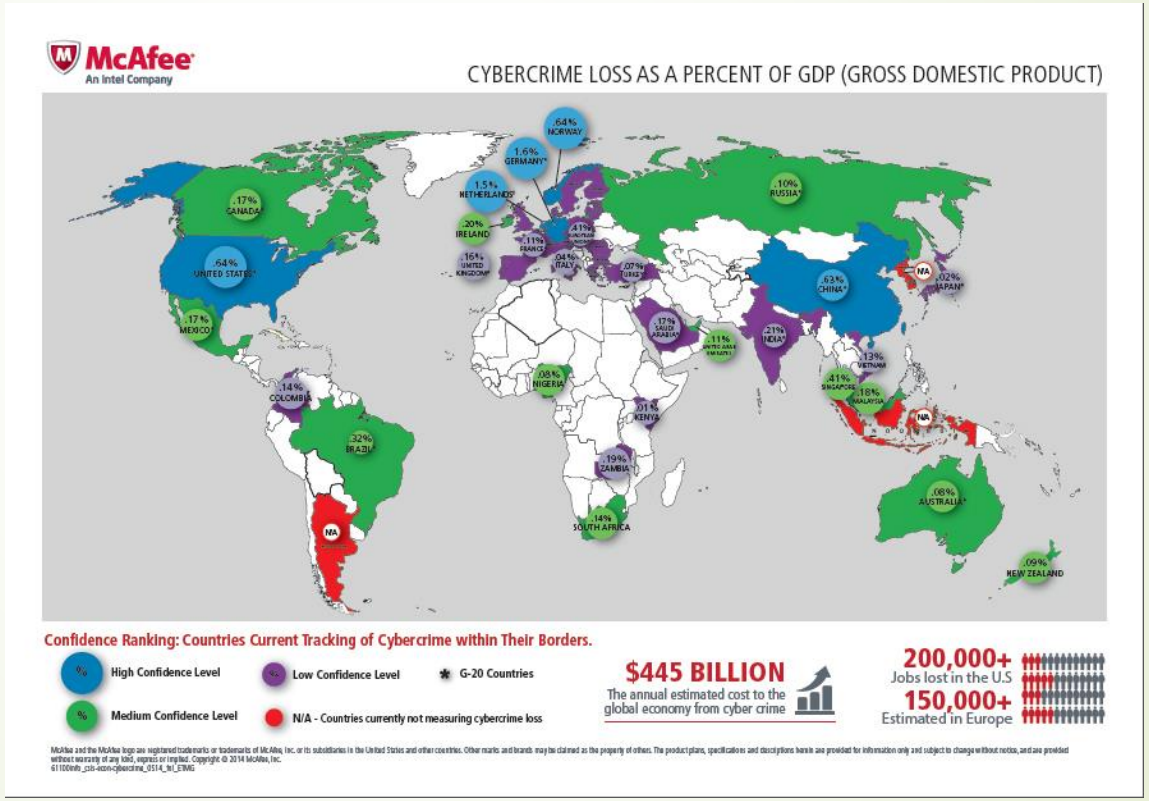
Bedrohung der freien digitalen Welt durch

- Staaten
  - USA
    - NSA-Skandal
    - Stuxnet
  - China
  - Russland
  - Deutschland
    - BND (Im Zusammenspiel mit den Amerikanern)
- Kriminelle Organisation
  - LulzSec, Unlimited Operation
- Einzelne Individuen
  - Aus Spaß
  - Finanzielle Interessen
  - Politische Motive

Eingesetzte Software und Methoden

- Worm (Wurm)
  - Stuxnet
  - Duqu
- Trojan (Trojaner)
  - Zeus
  - PRISM
- Zero-Day Exploits
- Backdoors
- Virus (größtenteils ersetzt durch Würmer)
- ***Social Engineering***

Wirtschaftlicher Schaden



Der Virus

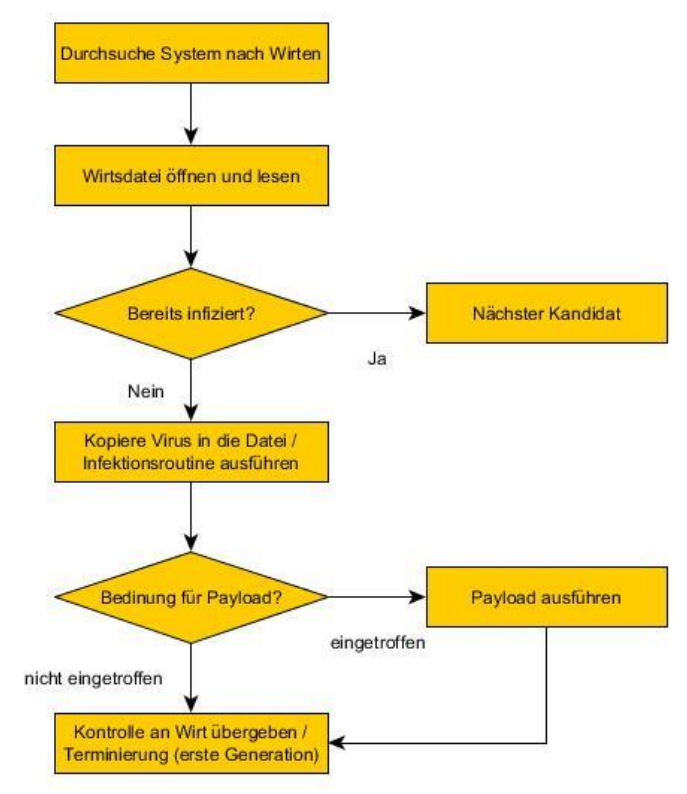
Definition

- “Computer viruses are small software programs that are designed to spread from one computer to another and to interfere with computer operation.” – Microsoft
- “A **computer virus** is a malware program that, when executed, replicates by inserting copies of itself (possibly modified) into other computer programs, data files, or the boot sector of the hard drive; when this replication succeeds, the affected areas are then said to be "infected“.” - Wikipedia

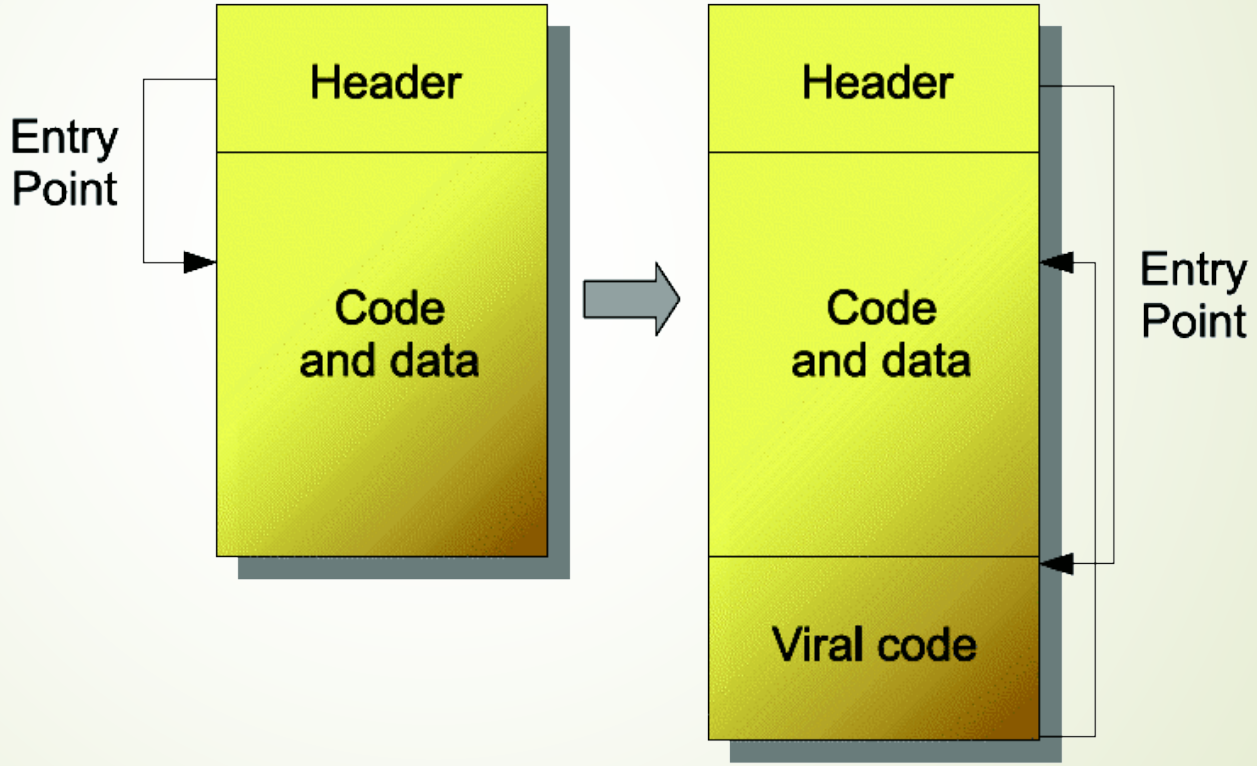
Abgrenzung zu anderer Malware

- Worm
  - Fast identisch
  - Worms benötigen keinen Wirt
  - Reproduktion durch Exploits und Emails
- Trojan
  - Als nützlich getarntes Programm
  - Benötigt keinen Wirt
- Medien und „Laien“ machen keine Abgrenzung
  - Malware = Virus (FALSCH!)

Funktionsweise



Datei vor und nach Infektion



Quelle: Advanced Polymorphic Techniques

Delta-Offset

```
        call delta
Delta:  pop ebp
        sub ebp, delta
```

Funktionsweise

Virus (erste Generation)

00400000: call 00400005

00400005: pop ebp

00400006: sub ebp, 00400005

Offset = delta – 00400005

= 00400005 – 00400005

= 0

Im Wirt

00600000: call 00600005

00600005: pop ebp

00600006: sub ebp, 00400005

Offset = delta – 00400005

= 00600005 – 00400005

= 00200000

Wirt

- Windows 32-Bit Executables (.exe)
- PE32-File Format
  - Header enthält Informationen über Datei
    - Entrypoint, Image Base, SizeOfCode, Data Directories
- Dynamic Link Librarys (.dll)
- Kernel32.dll
  - FARPROC WINAPI GetProcAddress(HMODULE hModule, LPCSTR lpProcName)
  - HMODULE WINAPI LoadLibrary(LPCSTR lpFileName)
- Adresse für kernel32.dll im Speicher können sich von Programm zu Programm oder Windows zu Windows unterscheiden

Kernel32.dll Suchmethode

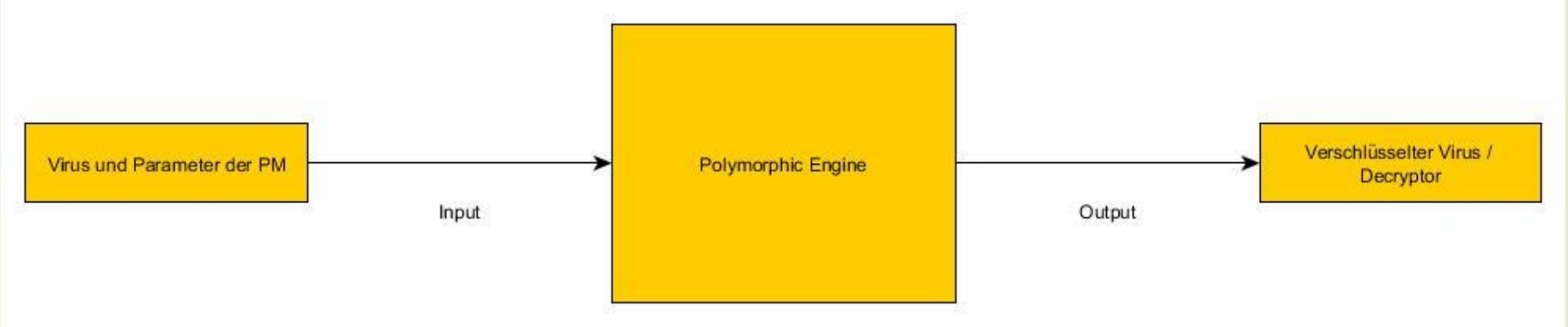
- Auslesen aus dem Process Environment Block
  - Liste der geladenen Module PEB->Ldr.InMemoryOrderModuleList.Flink
  - Dritter Eintrag kernel32.dll base address
- Verifiziert für
  - Windows 2000 SP4
  - Windows XP SP2
  - Windows XP SP3
  - Windows 2003 SP2
  - Windows Vista SP1
  - Windows 2008 SP1
  - Windows 7 RC1

Die Polymorphic Engine

Definition

- "A **polymorphic engine** (sometimes called **mutation engine** or **mutating engine**) is a computer program that can be used to transform a program into a subsequent version that consists of different code yet operates with the same functionality" - Wikipedia
- „However, a polymorphic virus adds these two components a third – a mutation engine that generates randomized decryption routines that change each time a virus infects a new program." – Symantec, striker.pdf

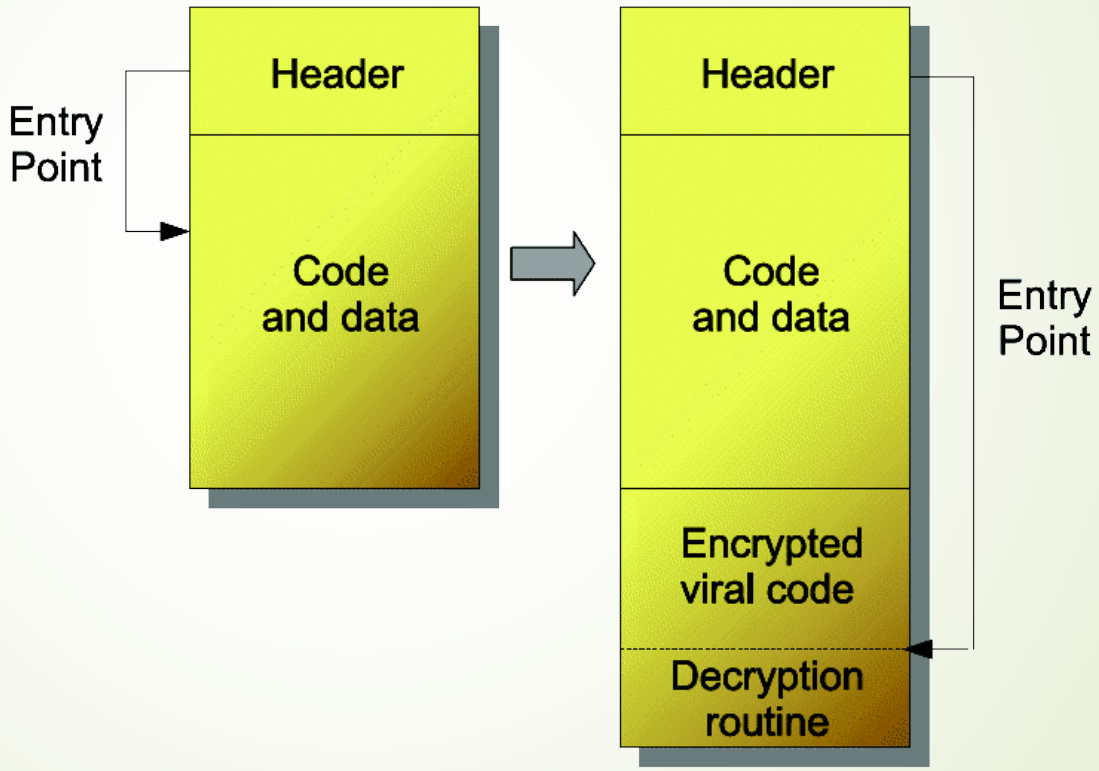
Funktionsweise



Funktionalitäten

- Verschlüsselung des Virus
- Entschlüsselung mittels Decryptor
- Mutation des Decryptors durch
  - Code Obfuscation (Verschleierung des Codes bzw. der Funktion)
  - Garbage Code (Instruktionen, die keinen Nutzen haben und nichts verändern)
  - Semantically Equal Code (Semantisch äquivalenter Code)
    - Mov eax, 0 = xor eax, eax
- Decryptor ist nicht verschlüsselt
- Jede Generation des Virus enthält eine eigene Version des Decryptors(Polymorphismus)
- Polymorphismus durch Parameter gesteuert

Zusammenspiel mit dem Virus



Quelle: Advanced Polymorphic Techniques

Warum Polymorphie?

- Antivirenprogramme suchen nach virusspezifischen Bytesequenzen
  - Verschlüsselung als Gegenmaßnahme
- Polymorphie soll das analysieren des Virus von Spezialisten erschweren
  - Garbage Code und Code Obfuscation als Methoden

Herangehensweise

Literatur

- Hauptsächlich englische Literatur
- The Giant Black Book of Computer Viruses von Mark Ludwig
- The Art of Computer Virus Research and Defense von Peter Szor
- Vxheaven.org
  - Großes Malware-Archive
  - Forum
  - Tutorials, Papers und Guides
- Diverse Paper

Tools

- FASM(flat assembler)
  - Einfacher Assembler mit simplen Interface
- OllyDbg
  - Sehr funktionsreiches Debugging Tool
- Latex für die Arbeit

Ziele der Bachelorarbeit

- Entwicklung eines einfachen polymorphen Virus
  - Einfacher Virus ohne anti-debugging, EPO (entry point obfuscation) oder andere Methoden gegen Antivirenprogramme (keep it simple)
  - Die Polymorphic Engine soll
    - Den Virus verschlüsseln mit mindestens zwei Verschlüsselungen
    - Einen Decryptor erzeugen mit
      - Garbage-Code
      - Semantically Equivalent Code
- Analyse des programmierten Virus und Vergleich zu Bestehenden
- Evaluation mittels der Entdeckungsrate bei Antivirenprogrammen

Zeitplan

- Literaturrecherche (1 Woche)
- Auswerten der Literatur (2 Wochen)
- Programmieren eines einfachen Virus (2 Wochen)
- Entwerfen und Programmieren einer funktionsfähigen Polymorphic Engine (4 Wochen)
- Zusammenführung von Virus und Polymorphic Engine zum polymorphen Virus (2 Wochen)
- Testen des Virus in einer Sandbox und Debbuging (1 Woche)
- Dokumentation finalisieren (2 Wochen)
- Zeitpuffer (2 Wochen)

Vielen Dank für Ihre Aufmerksamkeit!

Quellenverzeichnis

- Peter Szor: The Art of Computer Virus Research and Defense; Addison-Wesley Professional, 13. Februar 2005
- Mark Ludwig: The Giant Black Book of Computer Viruses, 2nd Edition; CreateSpace Independent Publishing Platform, 9. Februar 2009
- Philippe Beaucamps: Advanced Metamorphic Techniques in Computer Viruses; International Conference on Computer, Electrical, and Systems Science, and Engineering, 2007
- https://en.wikipedia.org/wiki/Polymorphic_engine, zuletzt aufgerufen am 19.11.2015
- Tokugawa Ieyasu: Delta Offset, Mai 2010; erhältlich auf http://vxheaven.org/lib/vti00.html, zuletzt aufgerufen am 19.11.2015
- Symantec: Understanding and Managing Polymorphic Viruses; https://www.symantec.com/avcenter/reference/striker.pdf, zuletzt aufgerufen am 19.11.2015

- Stephen Fewer: Blog, 19. Juni 2009; erhältlich auf http://blog.harmonysecurity.com/2009_06_01_archive.html, zuletzt aufgerufen am 19.11.2015
- Microsoft: Dynamic-Link Library Reference; erhältlich auf https://msdn.microsoft.com/en-us/library/windows/desktop/ms682602%28v=vs.85%29.aspx, zuletzt aufgerufen am 19.11.2015
- Wikipedia: Computer virus; erhältlich auf https://en.wikipedia.org/wiki/Computer_virus, zuletzt aufgerufen am 19.11.2015
- Wikipedia: Zeus (malware): erhältlich auf https://en.wikipedia.org/wiki/Zeus_%28malware%29, zuletzt aufgerufen am 19.11.2015
- McAfee: McAfee and CSIS: Stopping Cybercrime Can Positively Impact World Economies, 9. Juni 2014; erhältlich auf http://newsroom.mcafee.com/press-release/mcafee-and-csis-stopping-cybercrime-can-positively-impact-world-economies, zuletzt aufgerufen am 19.11.2015

- Wikipedia: Stuxnet; erhältlich auf https://de.wikipedia.org/wiki/Stuxnet#Duqu , zuletzt aufgerufen am 19.11.2015
- Wikipedia: Globale Überwachungs- und Spionageaffäre; erhältlich auf https://de.wikipedia.org/wiki/Globale_%C3%9Cberwachungs-_und_Spionageaff%C3%A4re , zuletzt aufgerufen am 19.11.2015
- Wikipedia: LulzSec; erhältlich auf https://de.wikipedia.de/wiki/LulzSec , zuletzt aufgerufen am 19.11.2015
- Roderic Broadhurst, Peter Grabosky, Mamoun Alazab, Steve Chon: Organizations and Cyber crime: An Analysis of the Nature of Groups engaged in Cyber Crime, IJCC Vol 8 Issue 1 January – June 2014; erhältlich auf http://www.cybercrimejournal.com/broadhurstetalijcc2014vol8issue1.pdf, zuletzt aufgerufen am 19.11.2015

- Wikipedia: Industrie 4.0; erhältlich auf https://de.wikipedia.org/wiki/Industrie_4.0 , zuletzt aufgerufen am 19.11.2015
- Wikipedia: Industrial Internet Consortium; erhältlich auf https://en.wikipedia.org/wiki/Industrial_Internet_Consortium, zuletzt aufgerufen am 19.11.2015
- Wikipedia: Internet of Things; erhältlich auf https://en.wikipedia.org/wiki/Internet_of_Things, zuletzt aufgerufen am 19.11.2015