Die Waffen des Cyberwar

Technische und politische Aspekte der offensiv militärischen Aktivitäten im Cyberspace

Thomas Reinhold,
IFSH - Institut für Friedensforschung und Sicherheitspolitik an der Universität Hamburg

reinhold@ifsh.de | cyber-peace.org

Gliederung des Vortrags

- Cyberspace: Abgrenzungs- und Definitionsprobleme
- Schadsoftware und Vorkommnisse seit 2010
- Zum Aufwand einer militärischen Cyberoperation
- Zusammenhänge und staatliche Akteure
- Trends in der digitalen Aufrüstung
- Politische Herausforderungen und Lösungsansätze
- Quellen

Zum Begriff Cyberspace

- *EU Cybercrime Convention (2001):*

  By connecting to communication and information services users create a kind of common space, called "cyber-space"

- *Cyber Security Strategy UK (2011):*

  “an interactive domain made up of digital networks that is used to store, modify and communicate information. It includes the Internet, but also the other information systems that support our businesses, infrastructure and services”

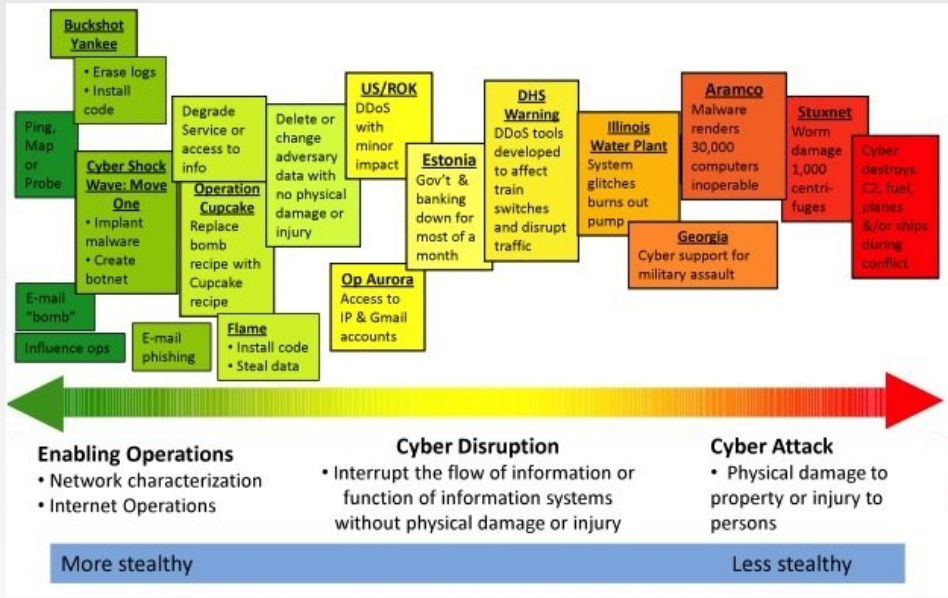
- Alle vernetzungsfähigen Computer & deren Infrastrukturen
- Alle Daten der Systeme, deren Austausch & Nutzeraktionen
- Vom Smartphone über Server bis zum Industrierechner

Abgrenzungs- und Definitionsprobleme

- Abgrenzung Krieg vs. Kriminalität
  - Cybercrime → Fragen nach Regelungen der internat. Strafverfolgung
  - Cyberwar → Fragen nach den politischen Motivationen der Akteure
  - Zentrales Problem: Welches Ausmaß einer nationalen Beeinträchtigung durch externe Cyberzugriffe entspricht einem kriegerischen Akt
- Kritische Infrastrukturen als maßgebliche Schwelle
  - BMI: Energieversorgung, ITK, Transport, Gesundheit, Wasser, Ernährung, Finanzwesen, Staat und Verwaltung, Medien
- Frage bleibt: „Was sind Cyberattacken?“

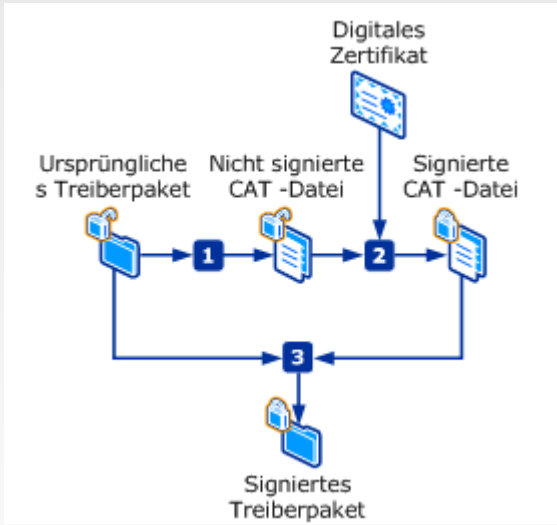
Abgrenzungs- und Definitionsprobleme II

- Aspekte bei der Bewertung
  - Ziel des Angriffs: Spionage, Sabotage oder Angriff mit Störwirkung
  - Identität und Motivation des Angreifers
  - Politische Rahmenbedingungen des Angegriffenen
- Kontinuums-Klassifikation
  - Gary D. Brown & Owen W. Tullos
  - (a) Access/Enabling Operations
  - (b) Cyber Disruption
  - (c) Cyber Attack



Schadsoftware - Technische Begriffe

- Command & Control Server (C&C-Server)
- Zero-day-exploit
  - unbekannte Sicherheitslücke
  - Ungeschütze Angriffsmöglichkeit
- Digitale Zertifikate
  - eindeutige digitale Unterschrift
  - Sicherheitsprüfung vor Installation system-kritischer Software
  - betrieblich gut geschützte Information



Schadsoftware - Typen und Klassifikationen

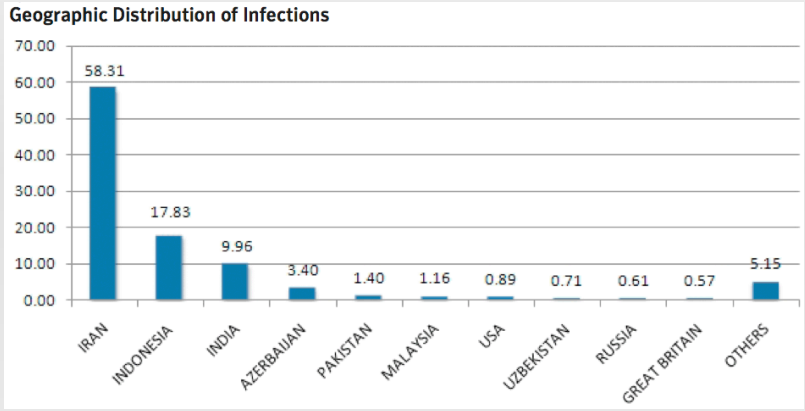
- Malware: Software mit unerwünschter, ggf. schädlicher Funktion
- Klassifikation nach Verbreitungsart, Schaden, Absicht, Zielsystem, Kontrollmöglichkeiten …
  - Viren — Reproduktion durch Einschleusen in Software
  - Würmer — Aktive Selbstverbreitung über Netzwerkdienste
  - Trojaner — Schadcode verborgen in scheinbar nützlicher Software
  - Botnetze — Verborgene Software auf Rechnern, die über Command-&-Control-Server ferngesteuert wird

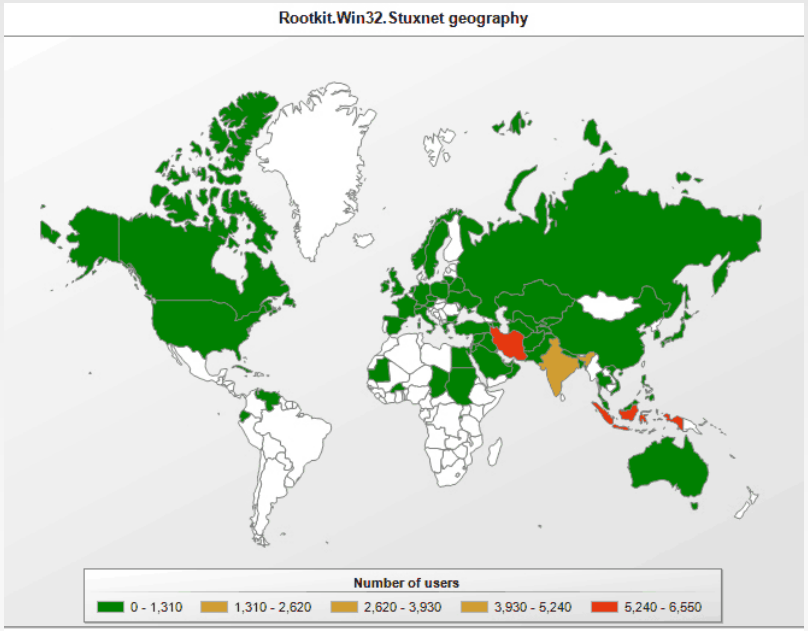
Vorkommnisse seit 2010 – Übersicht

Malware	Aktiv seit	Wirk-Ziel	Akteur
Stuxnet	06.2009	Schadwirkung iranische Atomanlagen	USA / Israel
Duqu	11.2010	gezielte Spionage IT-Strukturen	USA (?)
Flame	03.2010	„breite“ Spionage	USA
Gauss	09.2011	gezielte Spionage von Individuen	USA (?)
Rocra	05.2007	„High-target“ Spionage	Russland/China (?)
APT1	X.2005	„breite“, jahrelange Spionage	China (?)

Stuxnet - Keyfacts

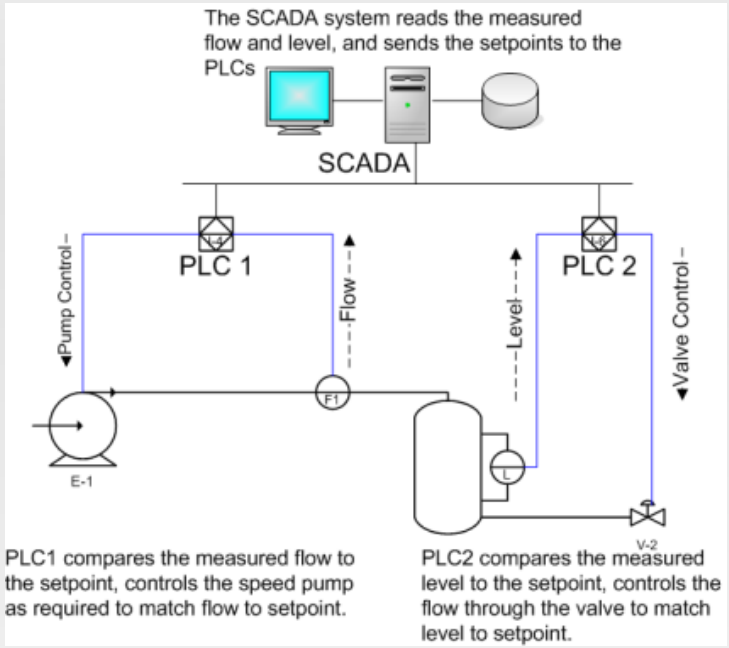
- entdeckt: Juni 2010
- sicher aktiv seit: Nov. 2007 / 2005
- Verbreitung: Industrieanlagen im Iran, Indonesien, Indien
- Infektion und Replikation
  - modifizierter USB-Stick
  - Windows-Netzwerkumgebung
- Hauptziel:
  - Schadwirkung
  - Zerstören von Uran-Zentrifugen





Stuxnet - Details

- Targeted Attack
  - für spezifische Hardware entwickelt (Siemens Step 7 SCADA)
  - für spezifische Anlage(n) entwickelt
- Überwindung des ”Air gap”
- Verwendung digitaler Zertifikate & vier Zero-day-exploits



- Millionen-Dollar-Projekt für Technologie, Entwicklung und SCADA-Testanlage
- Mehrjähriger Aufwand

Duqu – Keyfacts

- entdeckt: September 2011
- sicher aktiv seit: November 2010
- Verbreitung: 5 Technologie- und Forschungsorganisationen mit Sitz in Frankreich, Niederlande, Schweiz, Ukraine, Indien, Iran, Sudan, Vietnam

- Infektion und Replikation
  - modifiziertes WORD-Dokument
  - Windows-Netzwerkumgebung
- Hauptziel: gezielte Signal Intelligence (SigINT) und Spionage

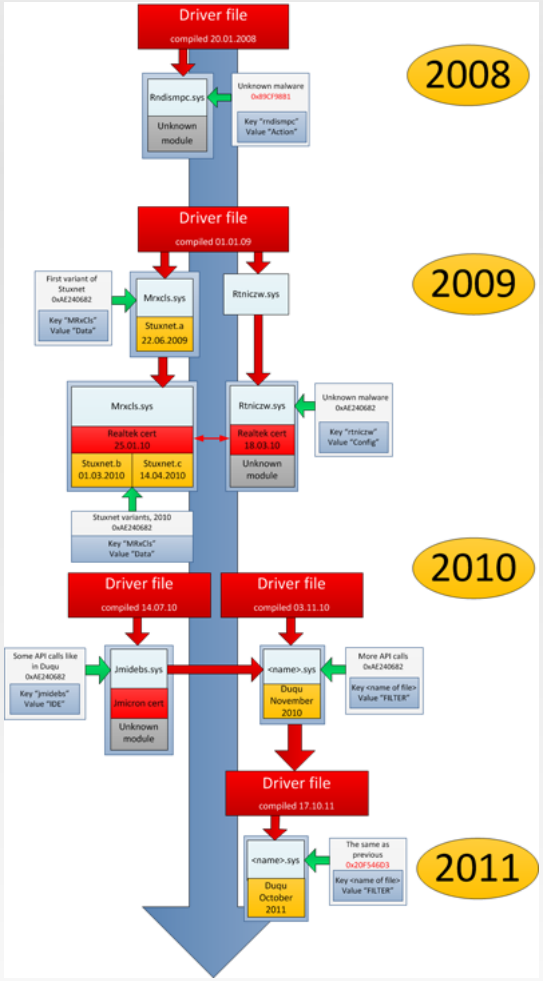
Duqu – Details

- Wirkung (Payload):
  - Aufnahme von Screenshots & Tastatureingaben
  - Sammlung von Netzwerk-Informationen
  - Suchen & Kopieren bestimmter Dateien
  - Eindeutige Identifikation jedes infizierten Systems
- Geringe Streubreite
  - 30-Tage Selbstabschaltung
  - Killswitch, im Oktober 2011 ausgelöst

Duqu – im Vergleich

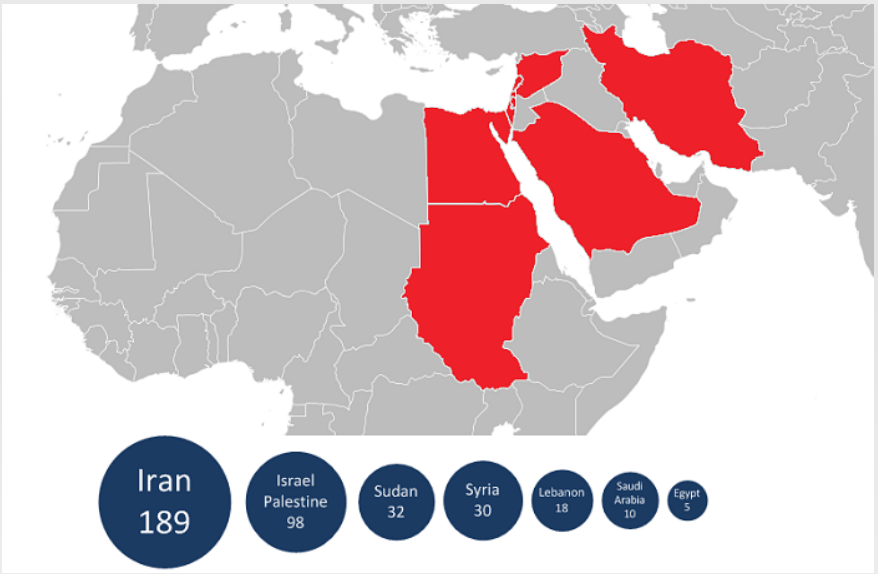
- Gesamtarchitektur zu Stuxent identisch
- Gleiches digitales Zertifikat wie bei Stuxnet

- Plattform „Tilded“ als Basis v. Duqu & Stuxnet
- „Tilded“ seit Ende 2007/08 entwickelt
- Wahrscheinlich weitere Projekte mit Tilded zwischen 2007 und 2011 realisiert



Flame – Keyfacts

- entdeckt: Mai 2012
- sicher aktiv seit: März 2010
- Verbreitung: Iran, Israel/Palästina, Libanon, Saudi-Arabien
- Infektion und Replikation
  - modifizierte USB-Sticks
  - Netzwerkumgebung und lokaler Windows-Update-Mechanismus
- Hauptziel: ”breite” SigINT und Spionage



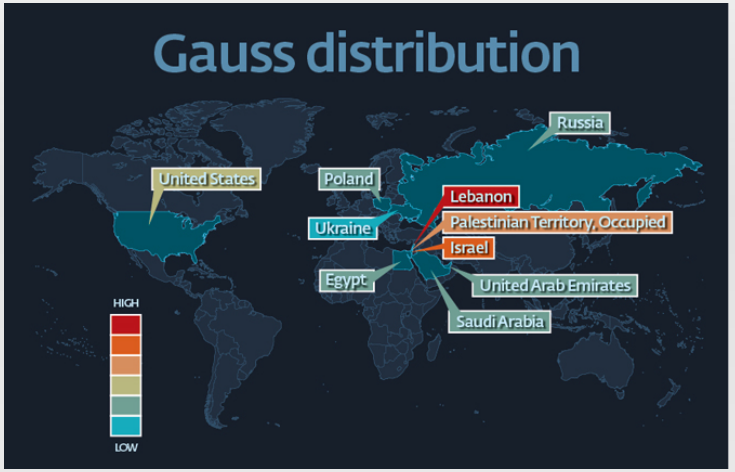
Flame – Details

- Payload ähnlich Duqu viele komplexe, nachladbare Module für Verschlüsselung, Datenbankzugriffe, Datenkompression
- Bluetooth-Geräte ausgelesen
- Killswitch im Juni 2012 ausgelöst
- C&C-Server noch aktiv und in Weiterentwicklung
- Teile von Flame bereits 2007 in Malware „Skywyper“ verwendet

Flame – im Vergleich

- Sehr viel komplexere Architektur & Code
- Verwendung zweier Zero-day-exploits wie bei Stuxnet
- Code-Verwandtschaft zwischen Stuxnet-Modulen und Flame
- Vermutlich parallel zu Tilded-Plattform entwickelt
- Gemeinsamer Ressourcenpool der Entwickler

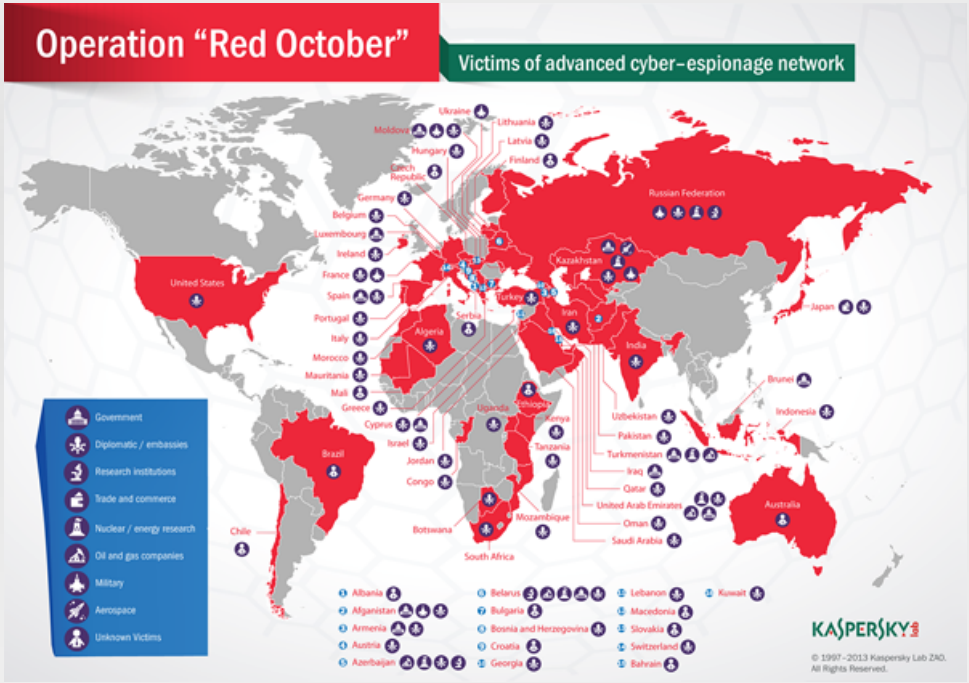
Gauss



- entdeckt: Juni 2012
- sicher aktiv seit: Sept. 2011
- Verbreitung: Libanon, Israel, Palästina
- Infektion: USB-Stick, keine Replikation
- Hauptziel: gezielte SigINT von Individuen
  - E-Mail & Social Media Zugängen, Browser-Verlauf, Cookies
  - Onlinebanking (regionale Banken, CitiBank, PayPal)
- Targeted Attack
- Nicht gelöscht, aber seit Juli 2012 im Schlafmodus
- Vermutlich auf Basis von Flame entstanden

Rocra – Keyfacts

- entdeckt: Oktober 2012
- sicher aktiv seit: Mai 2007
- Verbreitung: Spitzeneinrichtungen und diplomatische Vertretungen, insb. Osteuropa und Zentralasien
- Infektion und Replikation
  - gezielt thematische E-Mails
  - lokale Ausbreitung unter Ausnutzung gesammelter Informationen
- Hauptziel: Spionage von Daten höchster Vertraulichkeit
  - u.a. Daten eines populären Verschlüsselungsprogramm der EU/NATO

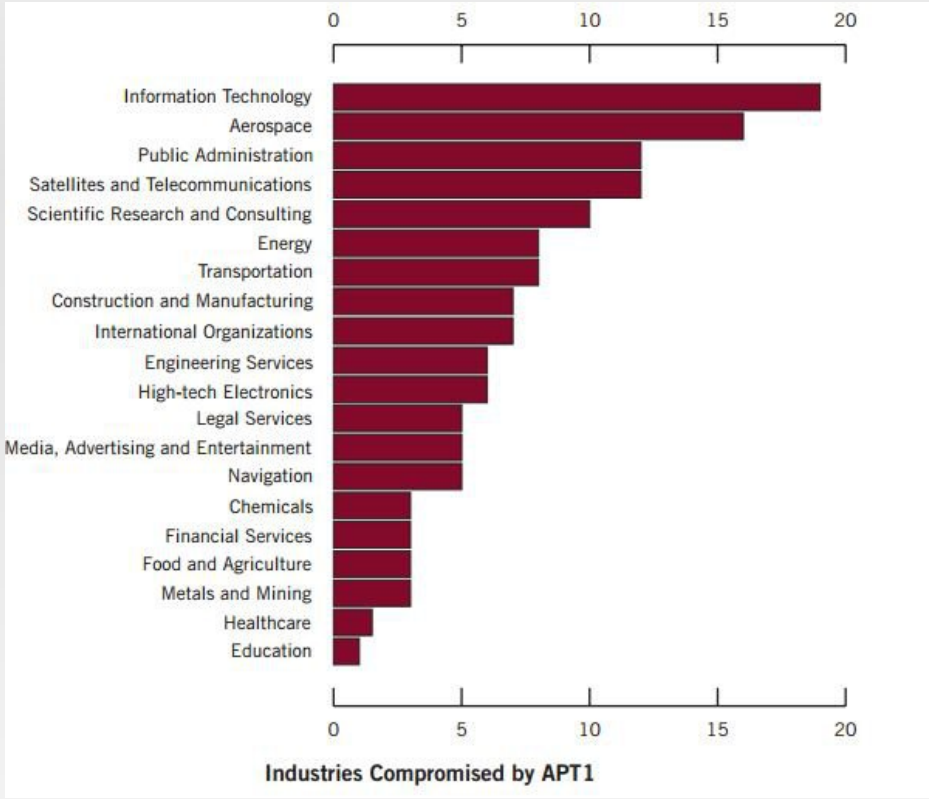


Rocra – Details

- Payload
  - Komplex und universell wie Flame
  - Daten auch von mobilen Datenträgern & angeschlossenen Telefonen
- Haupt-C&C-Server über Proxies verborgen
- Gesammelte Daten kontinuierlich weiter verwendet
- C&C-Server Anfang 2013 nach Veröffentlichung deaktiviert
- Chinesische und russische Bezeichnungen im Code

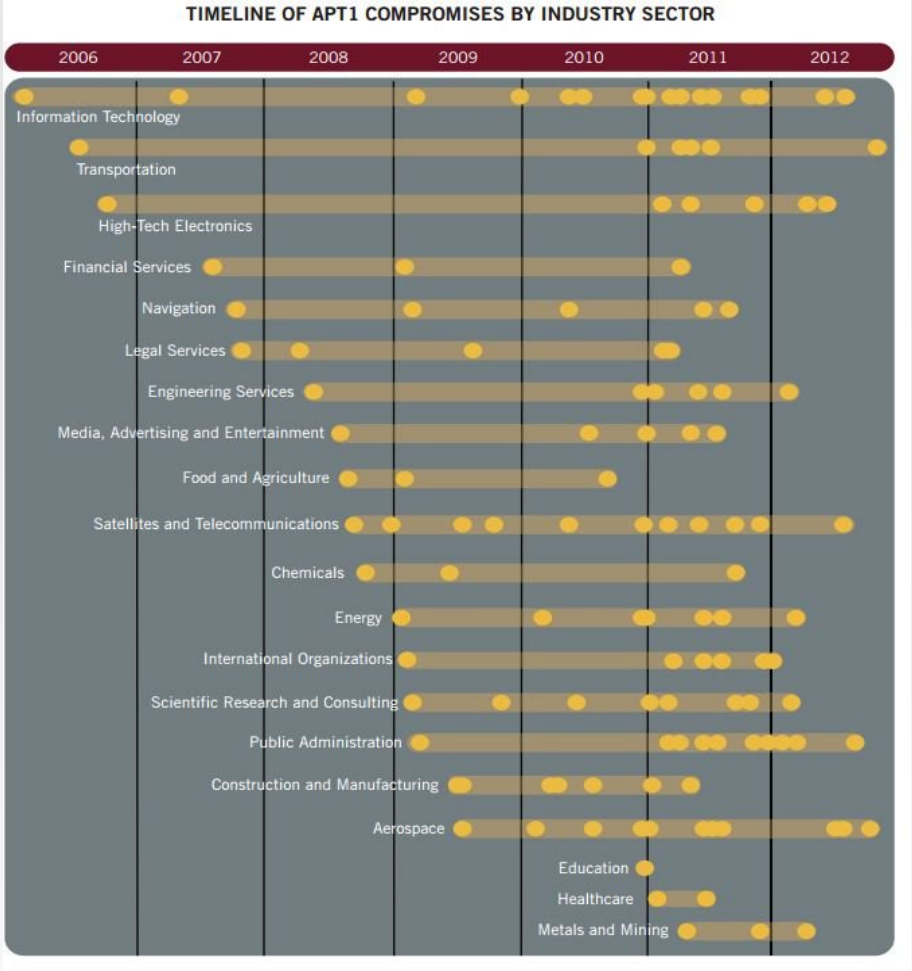
APT1 / PLA 61398

- Veröffentlicht: 02.2013
- sicher aktiv seit: X.2005
- Verbreitung:
  - 141 Einbrüche, bei 20 Haupt-industriezweigen USA, Kanada, UK
- Spionage-Netzwerk
- Eigenentwickelte Hacker-Tools
- Vermutlich chinesische Armee-Einheit 61398 für Cybersecurity, Pudong



APT1 / PLA 61398

- Veröffentlicht: 02.2013
- sicher aktiv seit: X.2005
- Verbreitung:
  - 141 Einbrüche, bei 20 Haupt-industriezweigen USA, Kanada, UK
- Spionage-Netzwerk
- Eigenentwickelte Hacker-Tools
- Vermutlich chinesische Armee-Einheit 61398 für Cybersecurity



Zum Aufwand einer militärischen Cyberoperation

- Anforderungen für einen erfolgreiche Cyberattacke
  - Sehr klares und genaues Missionsziel und nötige Befugnisse
  - Spezifische Zielinformationen, i.a.R. Vorfeldaufklärung nötig
  - Unbekannte Sicherheitslücken (Zero day exploits)
  - Hochgradig professionelles Entwicklungs/Test/Angriffs-Team
  - Beständkeit des Angriffes in Qualität und Dauer
- Zeitpunkt des 1. Angriffs → Vorteil wandert zum Verteidiger
- ~ Lebensspanne einer entdeckten Lücke: 500 Stunden
- Entwicklungsaufwand eines militär. Angriffs ca. 2 bis 5 Jahre

Zusammenhänge und staatliche Akteure I

- Urheberschaft von Stuxnet
  - NY Times 1.6.2012, (David E. Sanger)
  - Teil des Programms „Olympic Games“, gestartet 2006 von G.W.Bush
  - US-Gemeinschaftsentwicklung mit israelischem Militär
- Urheberschaft Flame
  - Washington Post 19.6.2012 (E. Nakashima, G. Miller , J. Tate)
  - Entwicklung des US-Militär für ein kontinuierliches Erforschen & Überwachen der Iranischen Netzwerke

Zusammenhänge und staatliche Akteure II

- 2 komplexe Entwicklungen mit gemeinsamen Ressourcen-Pool
  - Tilded (Stuxnet, Duqu)
  - Flame-Plattform (Flame, Gauss)
- Weitere unabhängige Akteure (Rocra, APT1/PLA 61398)
- staatliche Kooperationen (Stuxnet, Rocra)
- breites Spektrum an Cybertools
  - Spionage von IT-Infrastruktruren (Duqu)
  - Spionage von Individuen (Gauss)
  - „tiefgreifende“ Datenanalyse und Diebstahl (Flame)
  - Explizite Schadwirkung (Stuxnet)

Trends in der digitalen Aufrüstung

- *It makes sense "to take this on right now (..) Other countries are preparing for a cyberwar. If we're not pushing the envelope in cyber, somebody else will."* Richard M. George, former NSA cyber defense official
- Ausschreibung Cyberwar-Zentrale der US Air Force 08/2012
  - Cyberwarfare integraler Bestandteil militärischer Operationen
  - Attack: Stören, Unterbrechen, Manipulation, Zerstören fremder Systeme
  - Support: Schwächen finden, Ziele identifizieren, Informationssammlung für die Planung von Operationen, eigene Systeme schützen
  - Development: Möglichkeiten für aktive und defensive Cyberwarfare-Operationen entwickeln

Trends in der digitalen Aufrüstung II

- Bericht des BMVg an Verteidigungsauschuß vom 5.6.2012
  - Abteilung Computernetzwerkoperationen des Kommando Strategische Aufklärung seit 5 Jahren im Aufbau
  - *"Eine Anfangsbefähigung zum Wirken in gegnerischen Netzwerken wurde erreicht"*
  - *"Simulationen [würden] in einer abgeschlossenen Laborumgebung durchgeführt"*

Trends in der digitalen Aufrüstung III

- 33 Staaten mit militärischen Cyber-Programmen in Sicherheits- und Militärdoktrinen
  (J. Lewis 2011: Preliminary Assessment of National Doctrine and Organization)
  - USA: Department of Defence Cyber strategy (2011)
    handling the cyberspace as warfare domain (..) allows (DoD) to organize, train, and equip for cyberspace as we do in air, land, maritime, and space to support national security interests
    - Plan X (DARPA) 1.54 Mrd. $ von 2013 bis 2017 für „cyber-offense“
    - US Cyber command: 4000 zusätzl. Mitarbeiter in den nächsten Jahren
  - Russland: Erneuerte Militärdoktrin (2010)
    (equipping the armed forces includes) “the development of the forces and means of information warfare”
  - China: White Paper on National Defence (2004)
    (the *Army takes) „informationalization as its orientation and strategic focus”*

Politische Herausforderungen ...

- Politische Instabilität durch geheime Cyberwar-Programme
- Das Attributions-Problem
- Selbstverteidungsrecht nach dem „*ius ad bellum*“
- Rüstungskontrolle und Non-Proliferation (Dual Use)
- Kontrolle des Cyberspace und staatliche Souveränität
- Bedrohungspotential von Cybertools
- Verwundbarkeit nationaler Infrastrukturen
- Cyberattacken zwischenstaatlicher Akteure

… und Lösungsansätze

- Transparenz- und Vertrauensbildung
  - Analogien zu anderen Waffengattung (ABC) und Weltall-Konvention
  - Politische Seminare zu internationalen Cyberspace-Doktrinen
  - Bilaterale militärische Übungen
  - Verzicht auf den „First-Use“
  - Internationale Vernetzung und klare Hierarchisierung von CERTs (Computer Emergency Response Team)
  - Entwicklung von einheitlichen Standards und Bewertungsmaßstäben
  - UN-Cyberkonventionen und Verifikations-Maßnahmen
- Technische Lösungen
  - Cyberspace als „man made domain“ strukturell und funktionell gestaltbar

- Quellen
  - cyber-peace.org (im Aufbau)
  - searchsecurity.techtarget.com
  - securelist.com
  - heise.de/security
  - blogs.mcafee.com
  - kaspersky.com
  - symantec.com
  - „On the Spectrum of Cyberspace Operations“, Gary D. Brown and Owen W. Tullos
  - „Cybersecurity and Cyberwarfare - Preliminary Assessment of National Doctrine and Organization“, James Lewis, Center for Strategic and International Studies