Gibt es eine digitale Aufrüstung?

Eine Analyse der Trends, aktuellen Entwicklungen und Vorkommnisse im Cyberspace

Thomas Reinhold

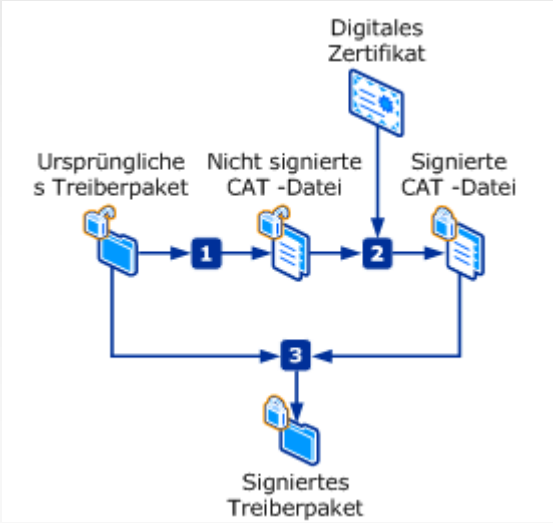
reit@hrz.tu-chemnitz.de

Gliederung des Vortrags

- Glossar
- Vorkommnisse seit 2010
  - Stuxnet
  - Duqu
  - Flame
  - Gauss
  - Mahdi
- Zusammenhänge und Akteure hinter der Software
- Trends und Einschätzung

Glossar

- Command & Control Server (C&C-Server)
- Zero-day-exploit
  - unbekannte Sicherheitslücke
- Digitale Zertifikate
  - eindeutige digitale Unterschrift
- Malware-Signaturen
  - für Antivirus-Software
  - Fingerabdruck von Programmcode

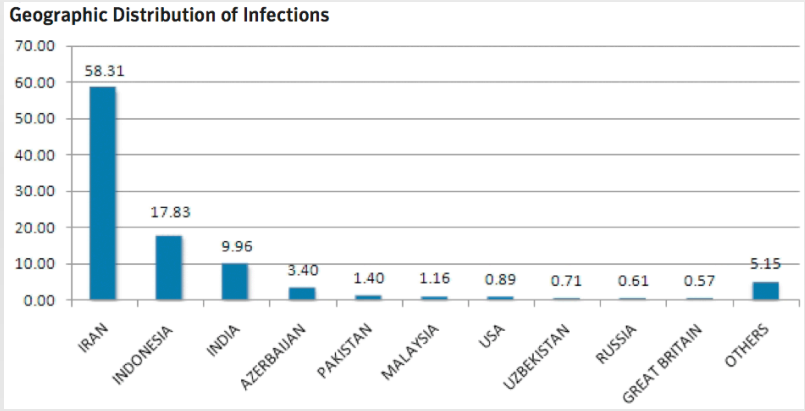


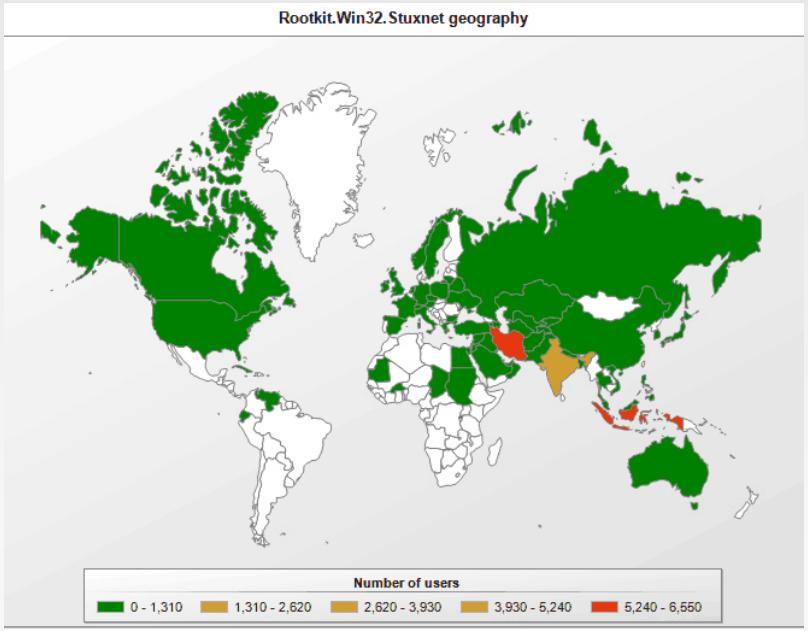
Vorkommnisse seit 2010 – Übersicht

Malware	Entdeckt	Sicher aktiv seit
Stuxnet	Juni 2010	Juni 2009
Duqu	September 2011	November 2010
Flame	Mai 2012	März 2010
Gauss	Juni 2012	September 2011
Mahdi	Juli 2012	September 2011

Stuxnet - Keyfacts

- entdeckt: Juni 2010
- sicher aktiv seit: Juni 2009
- letzte Neu-Infektion: August 2010
- Verbreitung: Industrieanlagen im Iran, Indonesien, Indien
- Infektion und Replikation
  - modifizierter USB-Stick
  - Windows-Netzwerkumgebung
- Hauptziel: Schadwirkung





Stuxnet - Details

- Targeted Attack
- Siemens Step 7 SCADA als Hauptziel
- 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
- letzte Aktualisierung: Oktober 2011
- 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 SigINT und Spionage

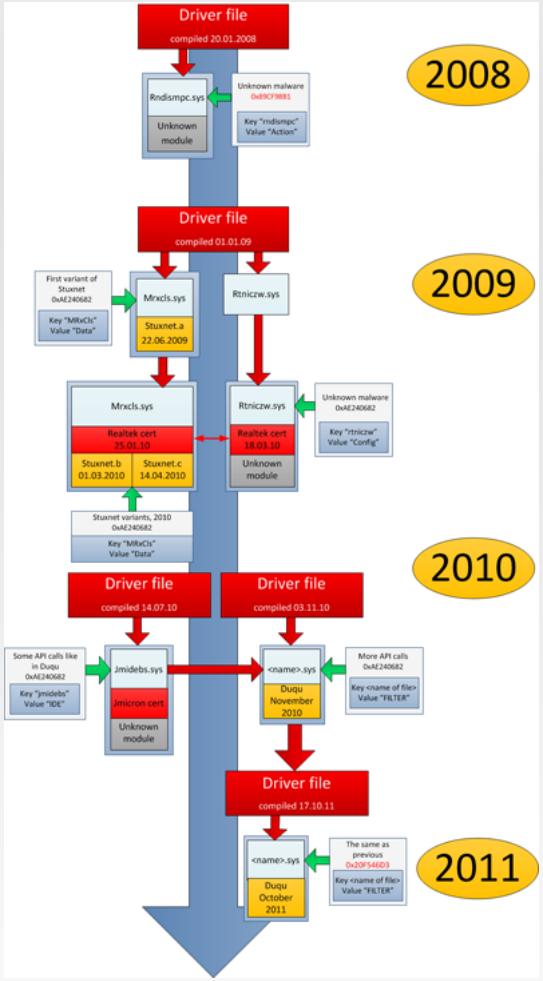
Duqu – Details

- Trojaner der direkt über C&C-Server gesteuert
- Erste Aktivitäten der C&C-Server seit November 2009
- Killswitch, im Oktober 2011 ausgelöst
- 30-Tage Selbstabschaltung
- Payload:
  - Aufnahme von Screenshots & Tastatureingaben
  - Sammlung von Netzwerk-Informationen
  - Datei-Zugriffe
  - Eindeutige Identifikation jedes infizierten Systems

Duqu – im Vergleich zu Stuxnet

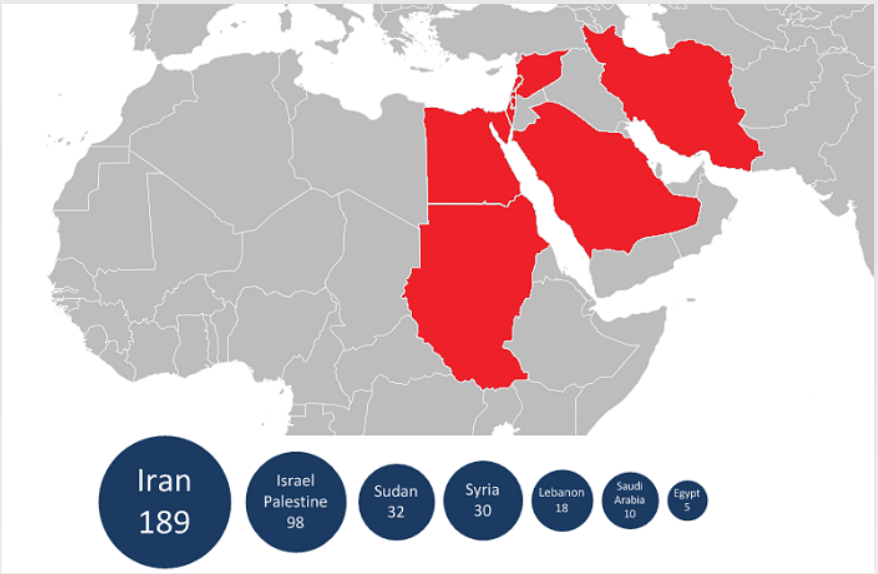
- Gesamtarchitektur der Malware identisch
- Gleiches digitales Zertifikat wie bei Stuxnet
- Weitere Treiber mit identischen Signaturen

- Plattform „Tilded“ als Basis v. Duqu & Stuxnet
- Tilded seit Ende 2007/Anfang 2008 entwickelt
- Wahrscheinlich weitere Projekte mit Tilded die zwischen 2007 und 2011 realisiert



Flame – Keyfacts

- entdeckt: Mai 2012
- sicher aktiv seit: März 2010
- letzte Aktualisierung: Mai 2012
- 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
- kein klassisches Verbergen sondern Tarnung
  als Datenbank-Anwendung
- Bluetooth-Geräte ausgelesen und als Data-Hub verwendet
- Killswitch im Juni 2012 ausgelöst
- Teile von Flame bereits 2007 in Malware „Skywyper“ entdeckt

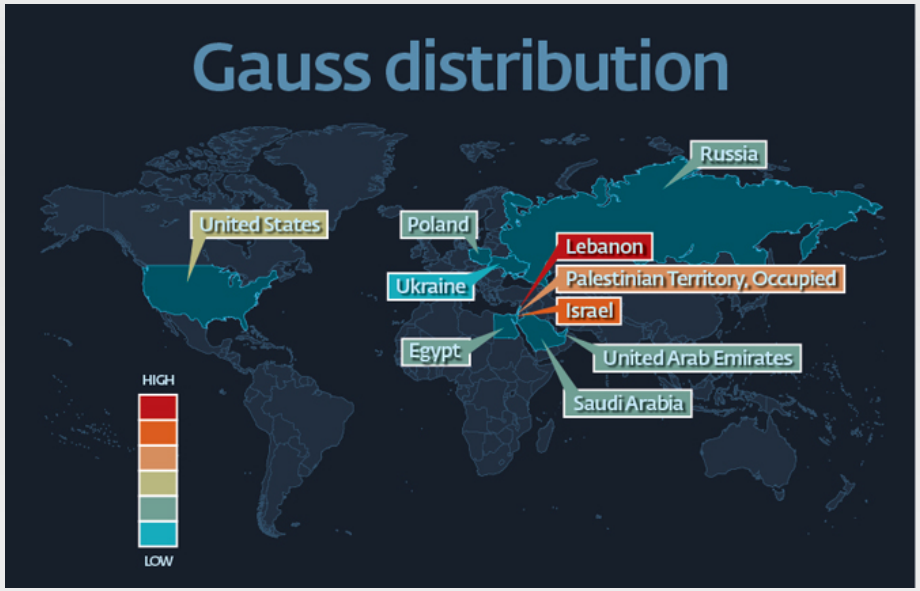
Flame – im Vergleich zu Stuxnet & Duqu

- Sehr viel komplexere Architektur & Code
- Verwendung zweier Zero-day-exploits wie bei Stuxnet
- Code-Verwandtschaft zwischen Stuxnet-Modulen und Flame
- Nicht auf aber vermutlich parallel zu Tilded-Plattform entwickelt

- C&C-Server noch aktiv und in Weiterentwicklung
- Drei weitere C&C-Client-Protokolle gefunden die bisher noch nicht in Malware aufgetaucht sind

Gauss – Keyfacts

- entdeckt: Juni 2012
- sicher aktiv seit: Sept. 2011
- letzte Aktivität: Juni 2012
- Verbreitung: Libanon, Israel, Palästina
- Infektion
  - modifizierte USB-Sticks
  - keine Replikation
- Hauptziel: gezielte SigINT und Spionage

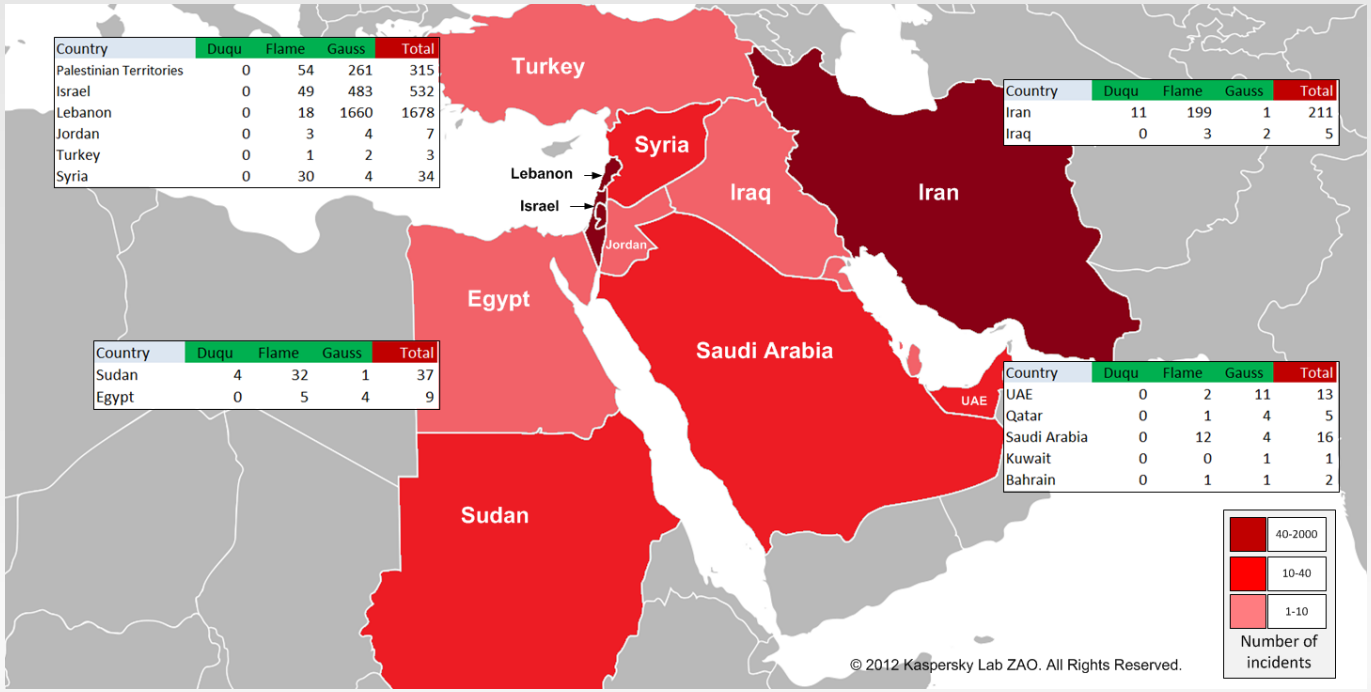


Gauss – Details

- Scheinbar auf Individuen gerichtet:
  - Spionage von E-Mail & Social Media Zugängen
  - Onlinebanking (nationale Banken, CitiBank, PayPal)
  - Browser-Verlauf, Cookies
- Payload & Module größtenteils verschlüsselt
- Juli 2012 C&C-Server offline, Gauss auf infizierten Systeme seitdem im Schlafmodus
- C&C-Server scheinbar auf hohes Datenaufkommen vorbereitet

Gauss – im Vergleich zu Stuxnet, Duqu & Flame

- Nutzt gleichen Zero-day-exploit wie Flame & Stuxnet
- Architektur & Code-Ähnlichkeiten zu Flame, gleiche Methodik in der Kommunikation mit den C&C-Servern
- Vermutlich auf Basis von Flame entstanden



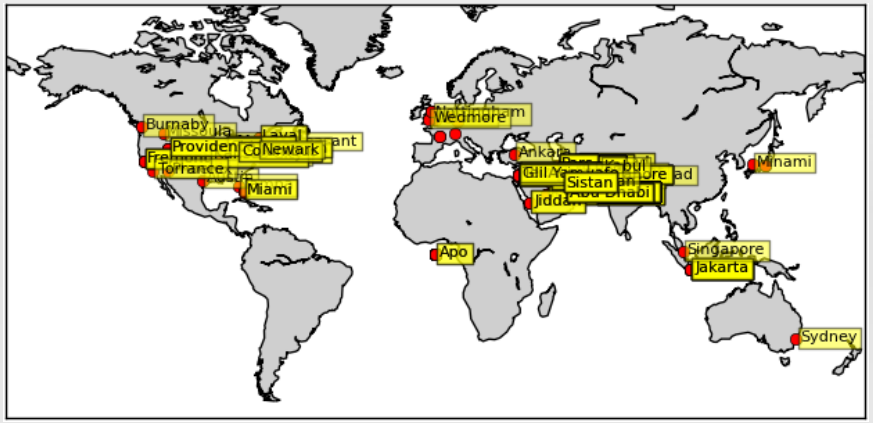
Country	Duqu	Flame	Gauss	Total
Palestinian Territories	0	54	261	315
Israel	0	49	483	532
Lebanon	0	18	1660	1678
Jordan	0	3	4	7
Turkey	0	1	2	3
Syria	0	30	4	34

Country	Duqu	Flame	Gauss	Total
Iran	11	199	1	211
Iraq	0	3	2	5

Country	Duqu	Flame	Gauss	Total
Sudan	4	32	1	37
Egypt	0	5	4	9

Country	Duqu	Flame	Gauss	Total
UAE	0	2	11	13
Qatar	0	1	4	5
Saudi Arabia	0	12	4	16
Kuwait	0	0	1	1
Bahrain	0	1	1	2

Mahdi – Keyfacts



- entdeckt: Juli 2012
- sicher aktiv seit: September 2011
- letzte Aktivität: Juli 2012
- Verbreitung: Iran, Pakistan, USA
  aus Finanz- und Wissenschaftsbereich sowie Verwaltung
- Infektion und Replikation
  - Modifizierte Powerpoint & Bilddateien
    mit religiösen/politischen Bezügen
- Hauptziel: Spionage und Datendiebstahl

Mahdi – Details

- Payload
  - Audio-Mitschnitte, Tastaturanschläge, Screenshots, E-Mail & Messaging
  - Suche & Manipulation von Dateien
- Keine Verwendung von Zero-day-exploits
- Malware in Delphi geschrieben
- Verwendung vieler persischer Bezeichnungen im Code
- Vermutlich noch aktive Weiterverbreitung

Mahdi – im Vergleich zu Stuxnet, Duqu, Flame & Gauss

- Keine Code-Ähnlichkeiten
- Simple aber effektive Mechanismen verwendet
- Keine hochrangige/kostspielige Entwicklung
- Ähnliche Payload-Ziele

Zusammenhänge und Akteure hinter der Software

- Mindestens zwei professionelle, komplexe Entwicklungen mit gemeinsamen Ressourcen-Pool
  - Tilded (Stuxnet, Duqu)
  - Flame-Platform (Flame, Gauss)
  - Vermutlich weitere unbekannte Projekte auf dieser Basis
- Mindestens ein weiterer unabhängiger Akteur (Mahdi)

Zusammenhänge und Akteure hinter der Software II

- Urheberschaft von Stuxnet
  - NY Times 1.6.2012, (David E. Sanger)
  - Teil des Programms „Olympic Games“, gestartet 2006 von G.W.Bush
  - US-Gemeinschaftsentwicklung (CIA, NSA) mit israelischem Militär
  - Absicht der Kontrolle von israelischen Initiativen durch Kooperation
- Urheberschaft Flame
  - Washington Post 19.6.2012 (E. Nakashima, G. Miller , J. Tate)
  - Kontinuierliches Erforschen & Überwachen der Iranischen Netzwerke
  - *“This is about preparing the battlefield for another type of covert action (...) Cyber-collection against the Iranian program is way further down the road than this.”*

Trends und Einschätzung

- Ausschreibung des Air Force Life Cycle Management Center (Cyberwar-Zentrale der US Air Force) von August 2012
- Cyberwarfare integraler Bestandteil militärischer Operationen
- Ziele der Ausschreibung
  - 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 und Einschätzung 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"*
- Professionalisierung & Kommerzialisierung
  - digitale Zertifikate, Air gap überwinden, Polymorphie der Verbreitung
  - Verschlüsselter, modularisierter Payload

- Quellen
  - blogs.mcafee.com
  - searchsecurity.techtarget.com
  - securelist.com
  - heise.de/security
  - kaspersky.com
  - symantec.com/connect
- Thomas Reinhold
  reit@hrz.tu-chemnitz.de