# Ausgewählte Angriffsvektoren

René “Lynx” Pfeiffer
Michael “MiKa” Kafka

DeepSec In-Depth Security Conference

# Worum geht's?

DEEPSEC

- Mögliche Gegenspieler & Motivationen
- Wege für Angriffe
- Schwachstellen & Risiken
- Schadensbegrenzung

# Sicherheit?

DEEPSEC

- *Integrität* der Verbindungs-/Gesprächsdaten
- *Vertraulichkeit* der Verbindungs-/Gesprächsdaten
- *Identität* der Gesprächsteilnehmer
- *Verfügbarkeit* der Infrastruktur

# Gegenspieler

# Hackers

DEEPSEC

- Ursprünge in den 1970er Jahren
- Telefonsysteme / „Phreaking“
- Boardsysteme mit Modemeinwahl
- Internet
- Motivation
  - Neugierde
  - Erkunden von Technologie
  - Spaß (unter Vorbehalt)

# Hackerhüte

DEEPSEC

- White Hats
  - Erkunden von Schwachstellen
  - Informieren, Absichern
  - Schaden wird möglichst vermieden
- Black Hats
  - Ausnutzen von Schwachstellen zu eigenem Vorteil
  - persönlicher Gewinn
  - Schaden wird in Kauf genommen/beabsichtig
- Grey Hats
  - Mischung aus White/Black Hat

# Script Kiddies



- *Script Kiddies* haben wenig Know-How
  - Einsatz „gefundener“ Tools
  - nicht zielgerichtet („targets of opportunity“)
- Motivation Anerkennung
  - „Hacks“ sind Trophäen
  - eigene Sprache/Kultur (z.B. *L33tsp33k*, …)
- Script Kiddies werden mitunter mißbraucht/ausgespielt
- kaum organisiert

# Hacktivismus

DEEPSEC

- politisch / religiös / kulturell motiviert
- bekannt seit Oktober 1989
  - WANK Wurm (Protest gegen Nukleartechnik)
- Zeichen setzen, Botschaften hinterlassen
- Ziele abhängig von Ausrichtung
- Auswirkungen ebenso

# Hacktivismus - Symptome

DEEPSEC

- Verändern von Webseiten (*Defacing*)
- Lahmlegen von Webseiten (*Web Sit-Ins*)
- E-Mail-Bomben
- „subversive“ Software
- Spiegeln von Webseiten (Antizensur)
- Geo-Bombing (über YouTube)
- anonymes Bloggen (z.B. Blog del Narco)

# Hacktivismus - Beispiele



THE Sun
Tuesday, 19 July 2011



HOME
NEWS
Weather
Forces
Sun City
Captain Crunch
Sun Says
Malaria No More
VIDEO
SPORT
Football
Dream Team
Cricket
F1 & Motorsport
SHOWBIZ
Bizarre
Film
Music
Biz Sessions
TV
BGT
Soaps
X Factor
TV Listings
WOMAN

## News



# Media moguls body discovered

By STAFF REPORTER

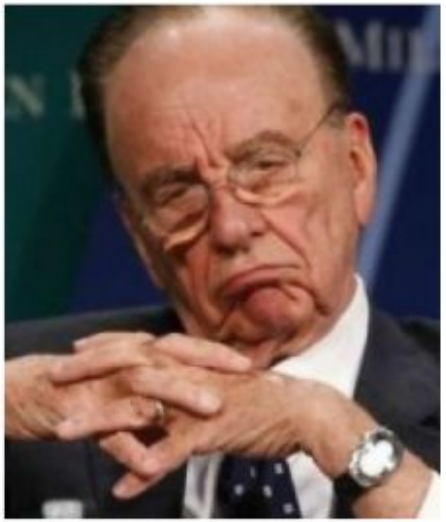
Published: Today

**Rupert Murdoch, the controversial media mogul, has reportedly been found dead in his garden, police announce.**

Murdoch, aged 80, has said to have ingested a large quantity of palladium before stumbling into his famous topiary garden late last night, passing out in the early hours of the morning.

"We found the chemicals sitting beside a kitchen table, recently cooked," one officer states. "From what we can gather, Murdoch melted and consumed large quantities of it before exiting into his garden."

Authorities would not comment on whether this was a planned suicide, though the general consensus among locals and unnamed sources



Media Mogul ... Rupert Murdoch

NEWS | SPORT | BIZARRE

**England mascot knifed to death**

EX England football mascot stabbed on Greek island in bust-up

# Cybercrime



- Profit
- digitales organisiertes Verbrechen
- Dienste und Werkzeuge käuflich
  - schlüsselfertig
  - Baukastenprinzip
- Waren sind Information

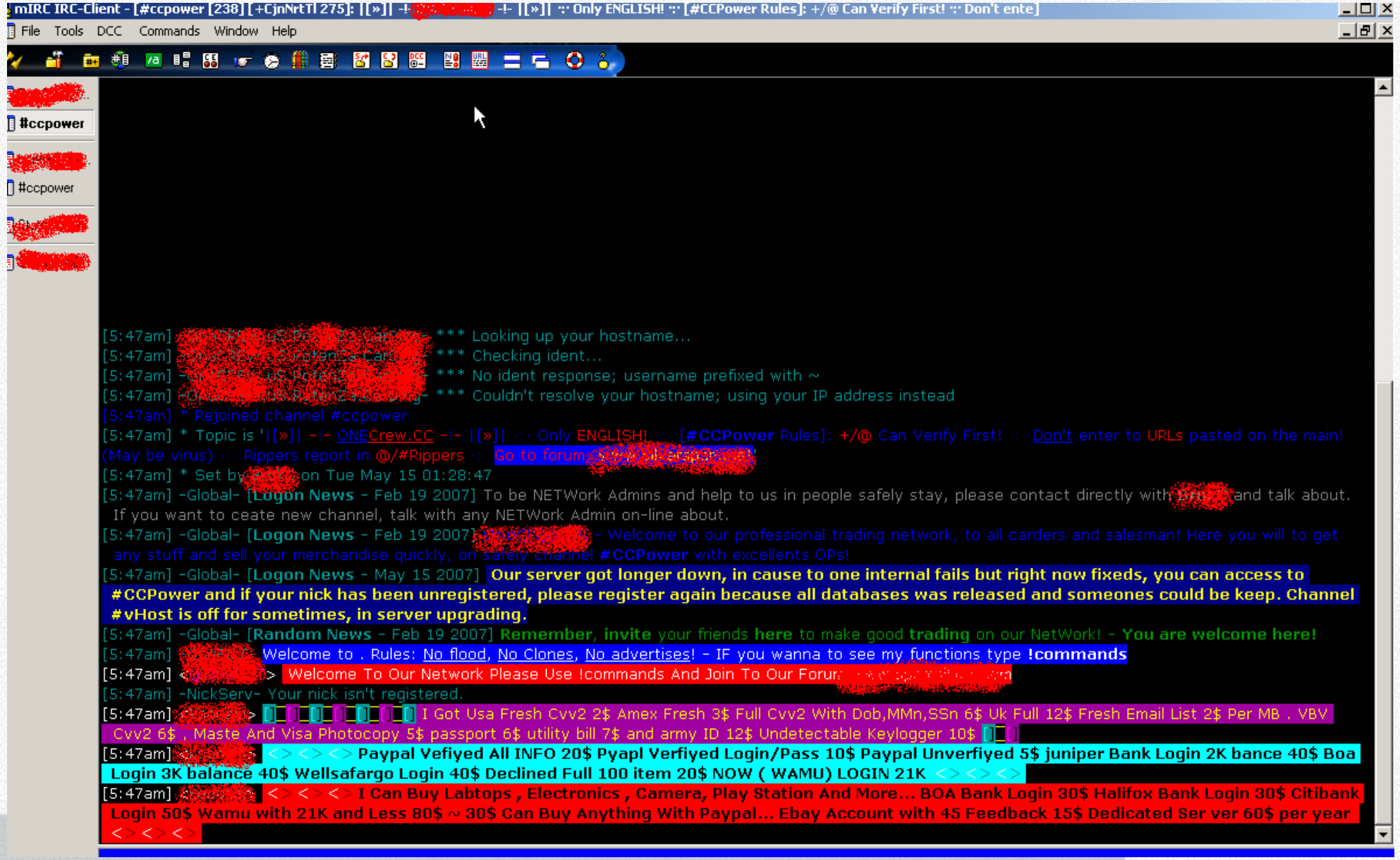
# Cybercrime - Symptome

DEEPSEC

- Betrug (*Phishing*, *Spamming*)
- Informationsdiebstahl
  - Konten, Kreditkarten
  - Logins, Paßworte, Identitäten
- Erpressung
- Spionage

# Cybercrime - Markplätze

DEEPSEC



# Zero Days / 0days

DEEPSEC

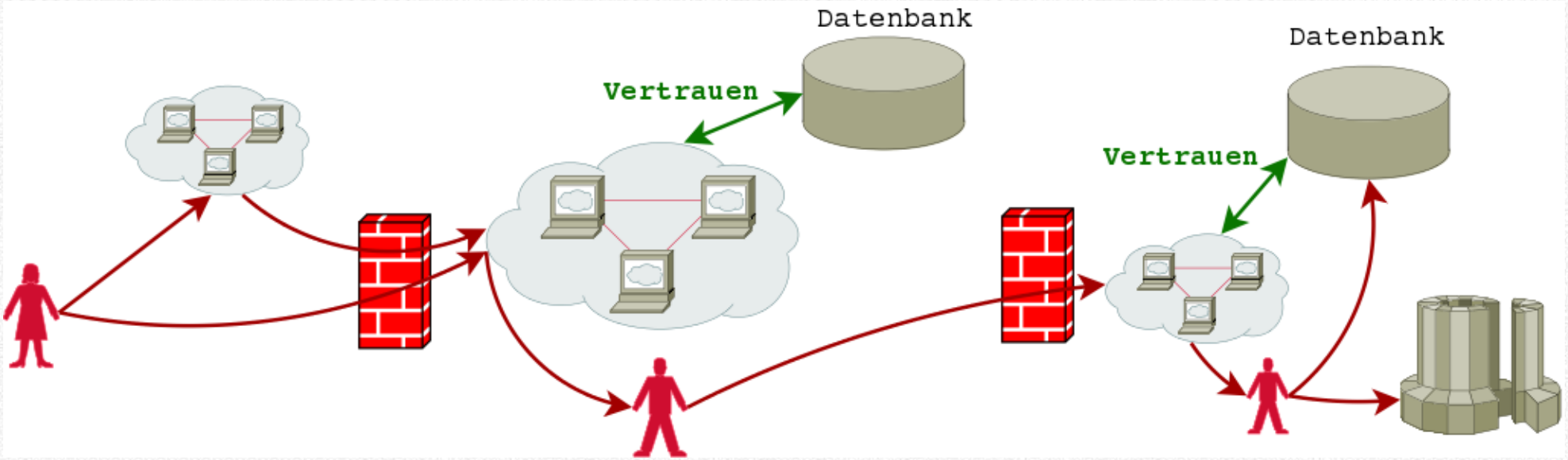
- *Zero Days* sind unveröffentlichte Schwachstellen
  - Schwachstellen (noch) nicht behoben
  - Verwendung in Angriffscode
- Zero Days werden gehandelt
  - Preise je nach Wirksamkeit / Plattformen
  - gute Zero Days werden sparsam eingesetzt
- Verteidigung
  - betroffene Systeme unzugänglich machen
  - gestaffelte Sicherheitsbarrieren

# Angriffsvektoren und -mittel

DEEPSEC

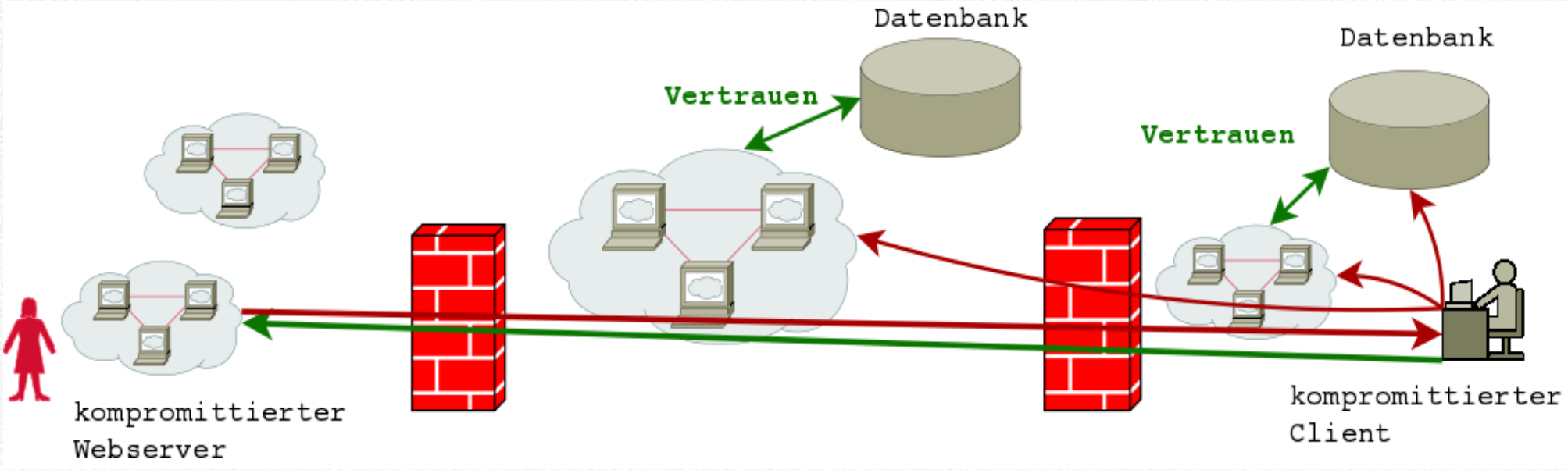
# Der lange Weg über Server





# Moderne Abkürzungen





# Desktops / Smartphones

DEEPSEC







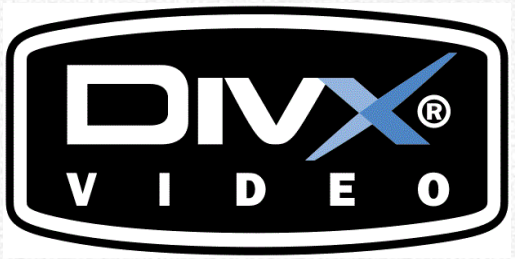











LibreOffice
The Document Foundation

# Desktops / Smartphones (2)



- sehr viel Software vorhanden
- reichhaltige Auswahl von Dokumentenformaten
- automatische Verknüpfungen
  - automatische Programmaufrufe
  - Ausführen von Code → Angriff
  - Netzwerk, USB-Geräte und Datenträger!
- Filter sind immer unvollständig

# Wege zum Desktop

DEEPSEC

# Browser und kurze Links

DEEPSEC

- Sicher oder unsicher?
  - http://t.co/W90EVyq
  - http://tpr.ly/nycn14
  - http://is.gd/mpcnRS
- Content Distribution Networks
  - wählen geographisch nächsten Server
  - verschiedene Ansichten „derselben“ Webseite
- Browser verstecken Details
- Browser stellen aktive Inhalte sofort dar

# Aktive Inhalte

DEEPSEC

- „Inline“ Dokumente (PDF, …)
- Adobe® Flash / Shockwave / AIR
- Microsoft® Silverlight
- Oracle Java™
- JavaScript
- Audio-/Videodaten
- 3D-beschleunigte Webseiten (WebGL)
- …

# Zombies



- Zombies sind infizierte Systeme
  - Infektion durch Viren / trojanische Pferde
  - Infektionsweg Web oder Nachrichten (E-Mail, …)
  - Systeme sind Computer (PCs, Server, Mobiltelefone, …)
- Zombies erhalten Kommandos
  - Command & Control (C&C) Kanal
  - zentrale Steuerung
  - Mechanismen für Updates

# Zombies - Symptome

DEEPSEC

- System kann keine Symptome zeigen
  - moderne Schadsoftware tarnt sich
  - Auffallen ist unerwünscht
- System kann seltsam reagieren
- Internetverbindung ist langsam/instabil
- Detektion meist möglich, abhängig von Schadsoftware

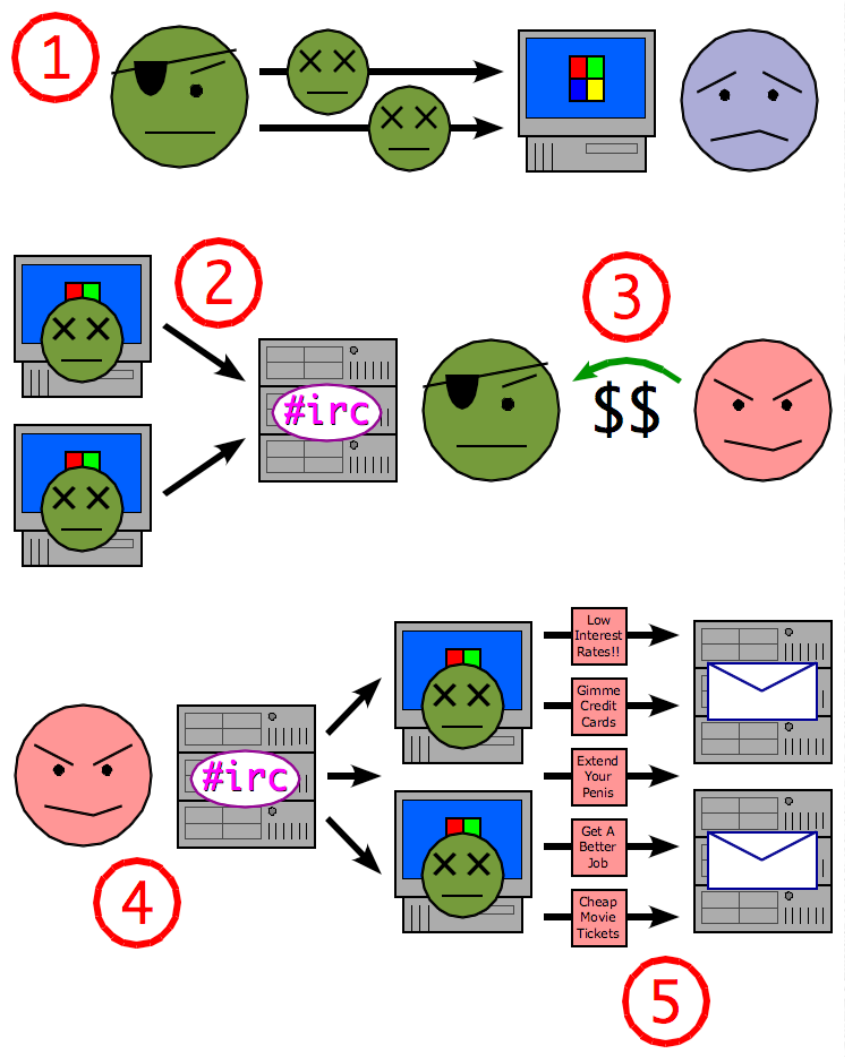
# Bot-Netzwerke

DEEPSEC

- Bot-Netzwerke bestehen aus Zombie-Systemen
  - von einigen 1.000 bis zu mehreren 1.000.000 Zombies
  - zentral gesteuert
- Bot-Netz-Betreiber vermieten Netzwerke für
  - Senden von E-Mail („Spam“)
  - Spionage (Zugänge, Passworte, …)
  - Überlasten von Diensten
- geschätzte 60 bis 150 Millionen Systeme sind in Bot-Netzen

# Zombie-Verbreitung





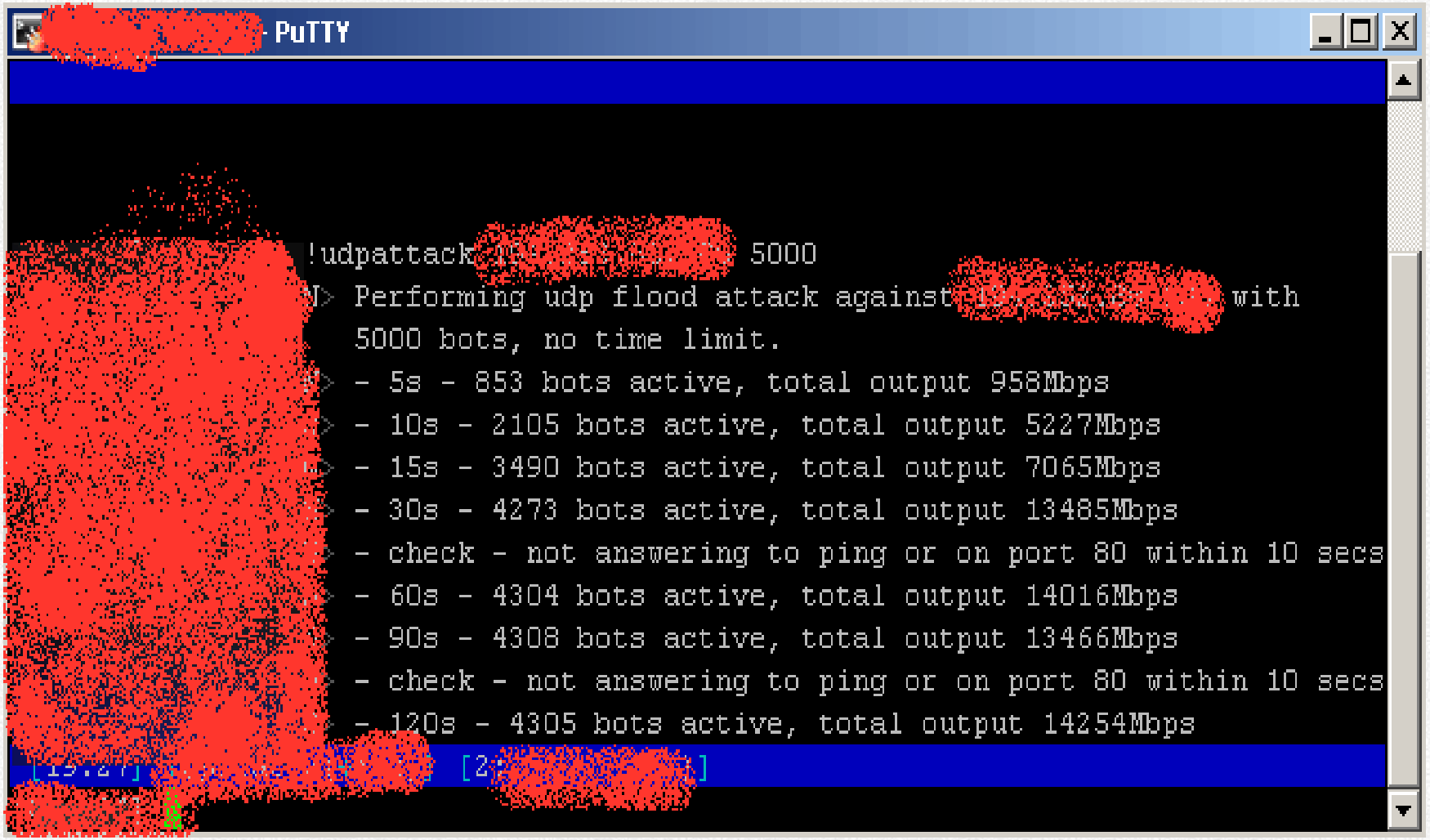
# Bot-Netzwerke (2)

DEEPSEC

| Bekannt seit | Abgeschaltet seit | Name | Maximale Botzahl | Milliarden Spammails pro Tag | Weitere Namen |
|---|---|---|---|---|---|
| Mai 2009 | Oktober 2010[4] | BredoLab | 30.000.000 [5] | 3,6 | Oficla |
| Mai 2009[6] | Dezember 2009[6] | Mariposa | 13.000.000[7] | ? | |
| Oktober 2008 | - | Conficker | 9.000.000[8] | ? | DownUp, DownAndUp, DownAdUp, Kido |
| 2006 | März 2011[9] | Rustock | 1.700.000 [10] | 44,1 [10] | RKRustok, Costrat |
| Januar 2007 [11] | - | Cutwail | 1.600.000 [12] | 74 [13] | Pandex, Mutant, Pushdo |
| März 2007 | - | Srizbi | 1.300.000 [14] | 60 [15] | Cbeplay, Exchanger |
| ? | - | Grum | 1.100.000 [11] | 39,9 | Tedroo |
| 2004 | - | Bagle | 780.000 [12] | 17,3 [12] | |
| August 2009 [10] | - | Maazben | 770.000 [10] | 4,8 [10] | |
| ? | - | Gheg | 500.000 [14] | 0,44 [12] | Tofsee, Mondera |
| ? | - | Kraken | 400.000 [16] | 9 | Kracken |
| ? | - | Bobax | 370.000 [10] | 14,6 [12] | Bobic, Oderoor, Cotmonger |
| Ende 2009 [17] | - | Lethic | 350.000 [17] | 2 [17] | |
| August 2009 | - | Festi | 220.000 [12] | 1,4 [12] | |
| ? | - | Mega-D | 180.000 [11] | 10 | Ozdok |
| ? | - | Torpig | 180.000 [18] | ? | Sinowal, Anserin |
| Januar 2007 | - | Storm | 160.000 | 3 | Nuwar, Peacomm, Zhelatin |
| ? | - | Donbot | 125.000[19] | 0,8 | Buzus, Bachsoy |
| November 2008 | Februar 2010[20] | Waledac | 80.000 | 1,5 | |
| März 2009 [10] | - | Cimbot | 48.000 [10] | 1,9 [10] | |

# Bot-Netzwerk in Aktion





# Denial of Service (DoS)

DEEPSEC

- Lahmlegen von Systemen durch
  - Erschöpfen von Resourcen
  - Ausnutzen von Fehlern in Software/Protokollen
- kann Nebeneffekt sein
- kann weitere Schritte verdecken
  - Ablenkungsmanöver
  - Ausnutzen von Abhängigkeiten
  - Vorbereitung weiterer Attacken

# Distributed Denial of Service

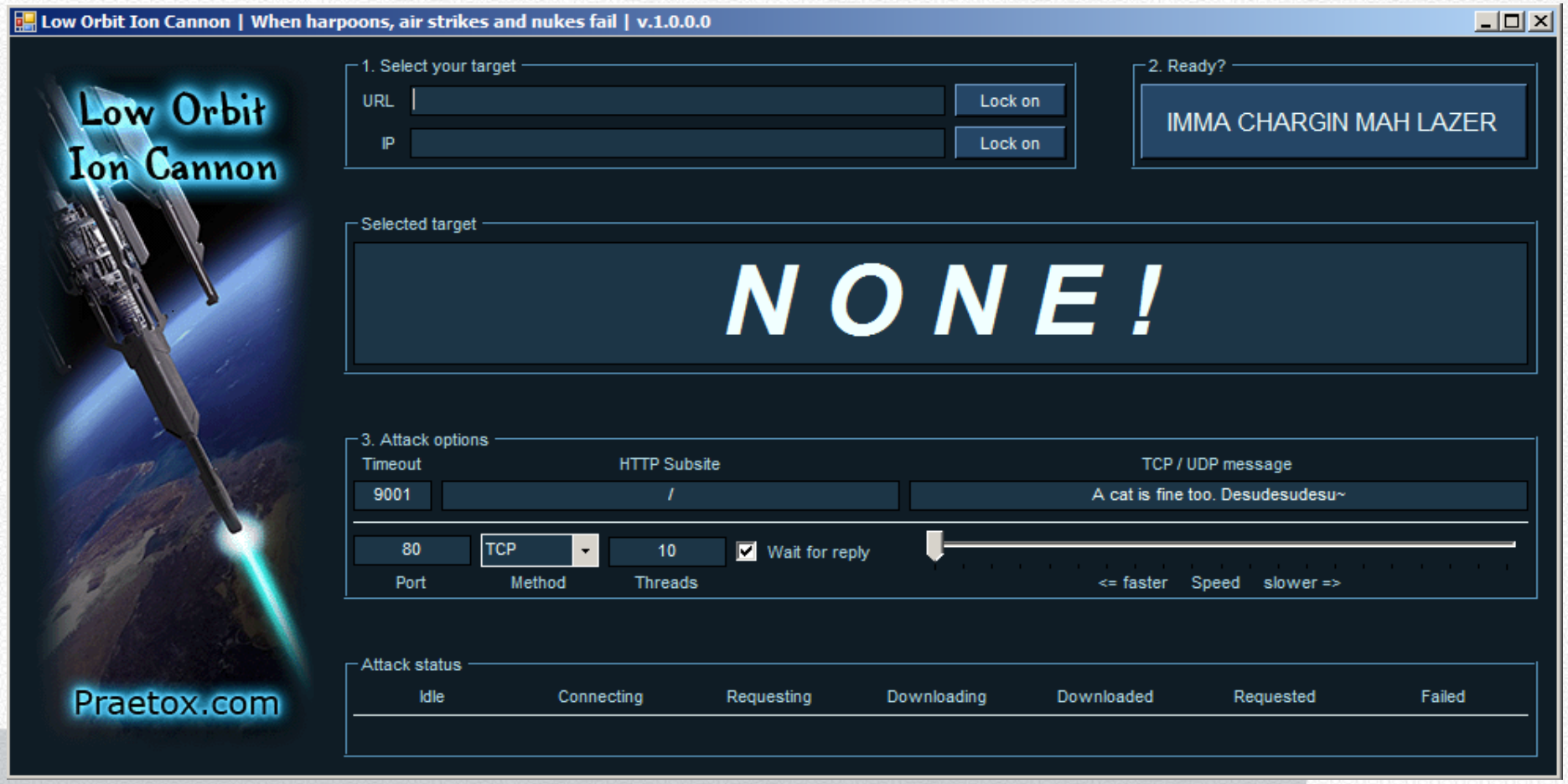


- DoS mit vielen verschiedenen Quellen
- koordinierte Attacke
  - Quellen müssen synchronisiert sein
  - Quellen agieren auf Kommandos
- sehr wirkungsvoll gegen viele Ziele
- Verteidigung nur im Verbund möglich
  - ISP muß mithelfen
  - Einsatz Content Distribution Networks (CDNs)

# „Low Orbit Ion Cannon“

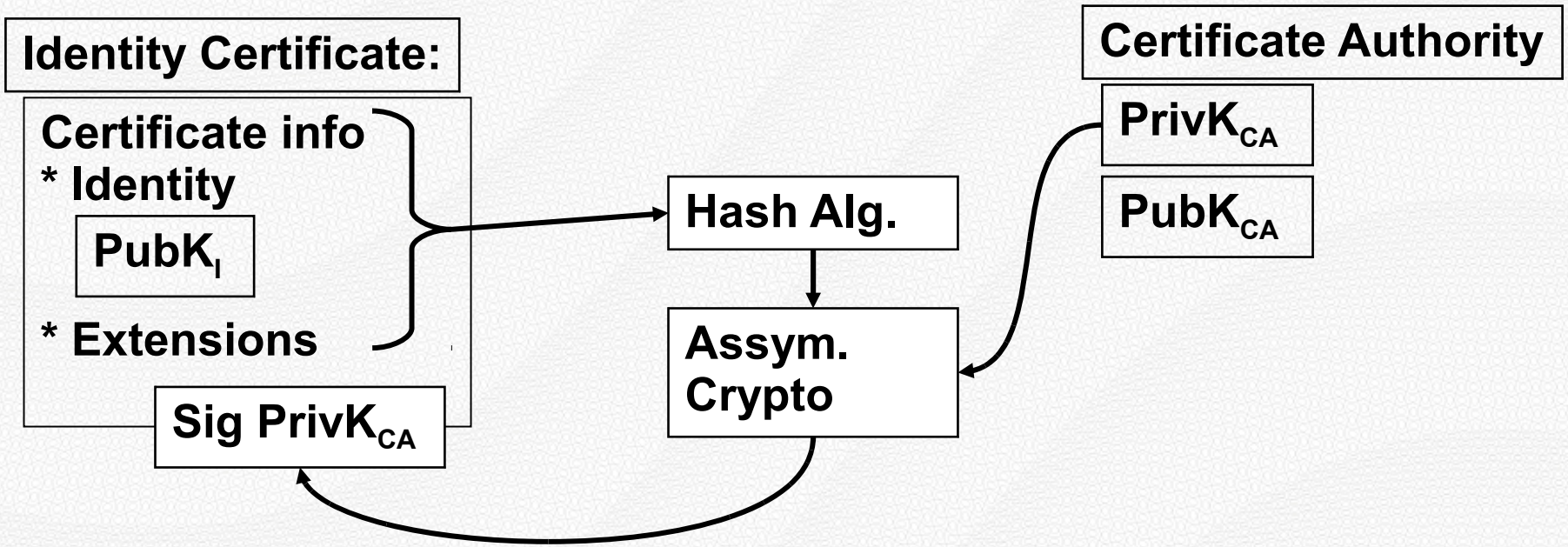


- Tool oft eingesetzt von Anonymous (seit 2006)
- Ziel sind meist Webserver



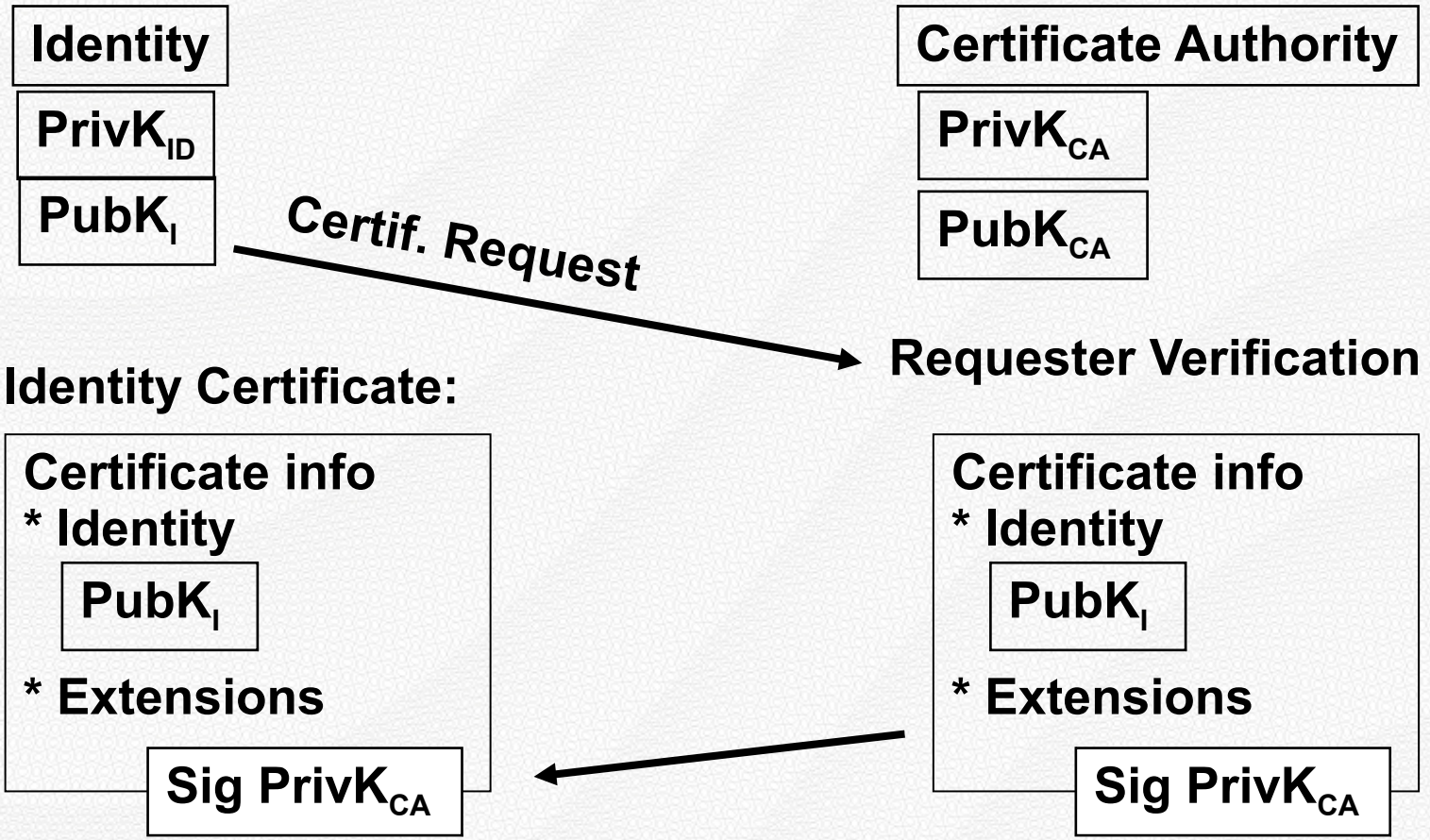
# Digitale Zertifikate

DEEPSEC


Identity Certificate:
Certificate info
* Identity
PubK$_I$
* Extensions
Sig PrivK$_{CA}$
Hash Alg.
Assym. Crypto
Certificate Authority
PrivK$_{CA}$
PubK$_{CA}$

# Zertifikatsausstellung





# Zertifikat Verifikation 1)



**Certificate Authority**

**$PrivK_{CA}$**

**$PubK_{CA}$**

Self-signed Certificate:

**Certificate info**
*** Identity**
**$PubK_{CA}$**
*** Extensions**
**Sig $PrivK_{CA}$**

**Identity**

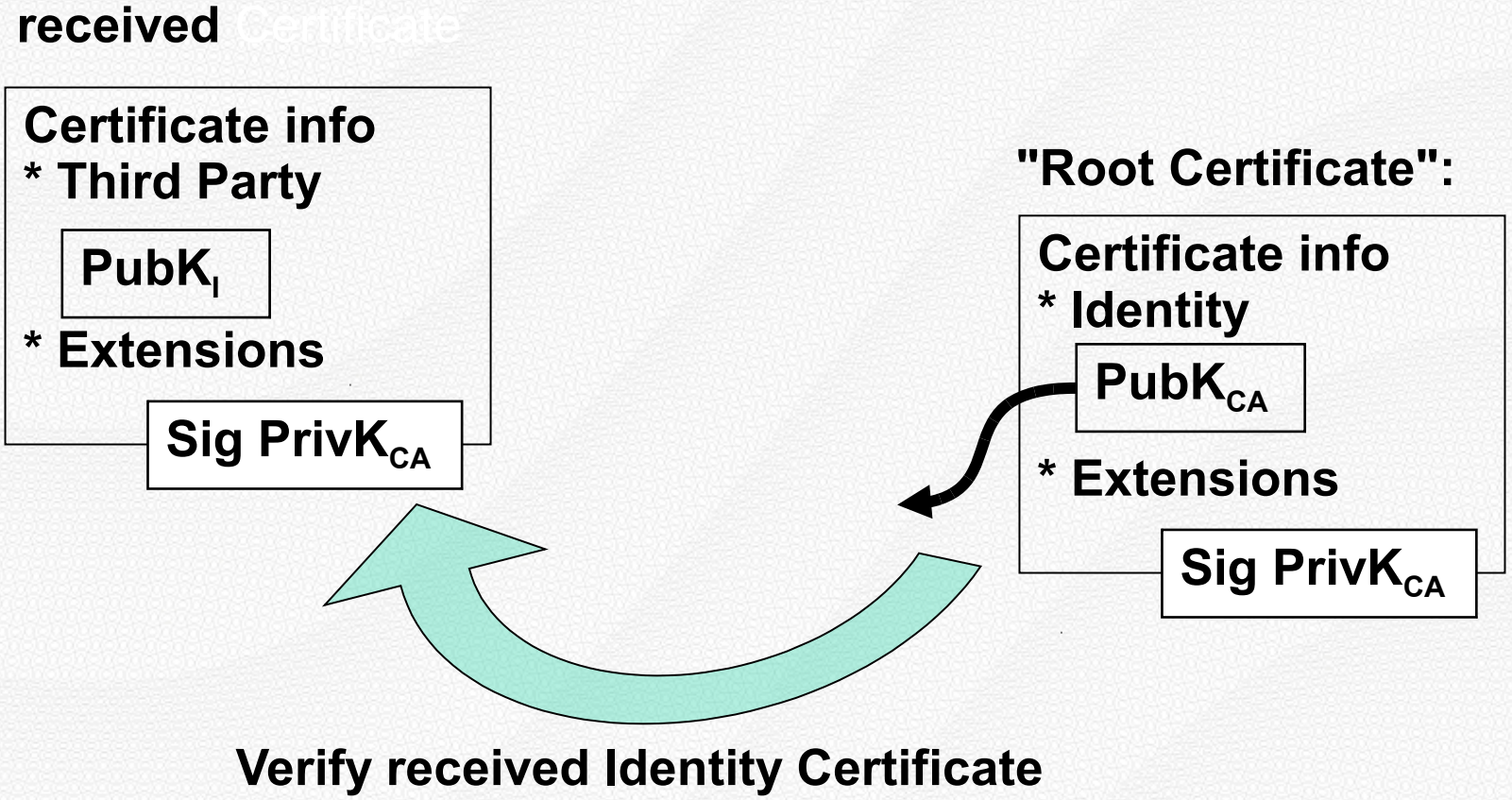
**Requests "Root Certificate":**

**Certificate info**
*** Identity**
**$PubK_{CA}$**
*** Extensions**
**Sig $PrivK_{CA}$**

**received**

# Zertifikat Verifikation 2)





# Zertifikat Verifikation: Probleme



<u>Unklarheiten:</u>

Welchen Root Zertifikaten vertraue ich?

Wo hat die Identity signieren lassen?

Hat die CA sauber verifiziert?

Grundsätzliches Vertrauen

Überprüfung Nachfrage nur explizit

CRL bzw. OCSP

# Vorfälle beim Signieren



Verisign, Januar 2001

Signiert zwei Zertifikate "für" Microsoft

Request war gefälscht

Zertifikat für "Code Signing"

Zwei Monate unentdeckt:

"In mid-March 2001, VeriSign, Inc., advised Microsoft that on January 29 and 30, 2001, it issued two VeriSign Class 3 code-signing digital certificates to an individual who fraudulently claimed to be a Microsoft employee…"

# Falsch ausgestellte Zertifikate: DEEPSEC

Falsch ausgestellte Zertifikate:

Erfolgreiche MitM Attacke

Wird nicht erkannt

Keine Verknüpfung Zwischen CA und Identity

Risiken z.B. Etisalat, Arabische Emirate:

Seit 2005 als "Trusted Root" erkannt (Cybertrust)

Schlechte Erfahrungen mit Blackberry 2009

Gilt für hunderte weitere Organisationen...

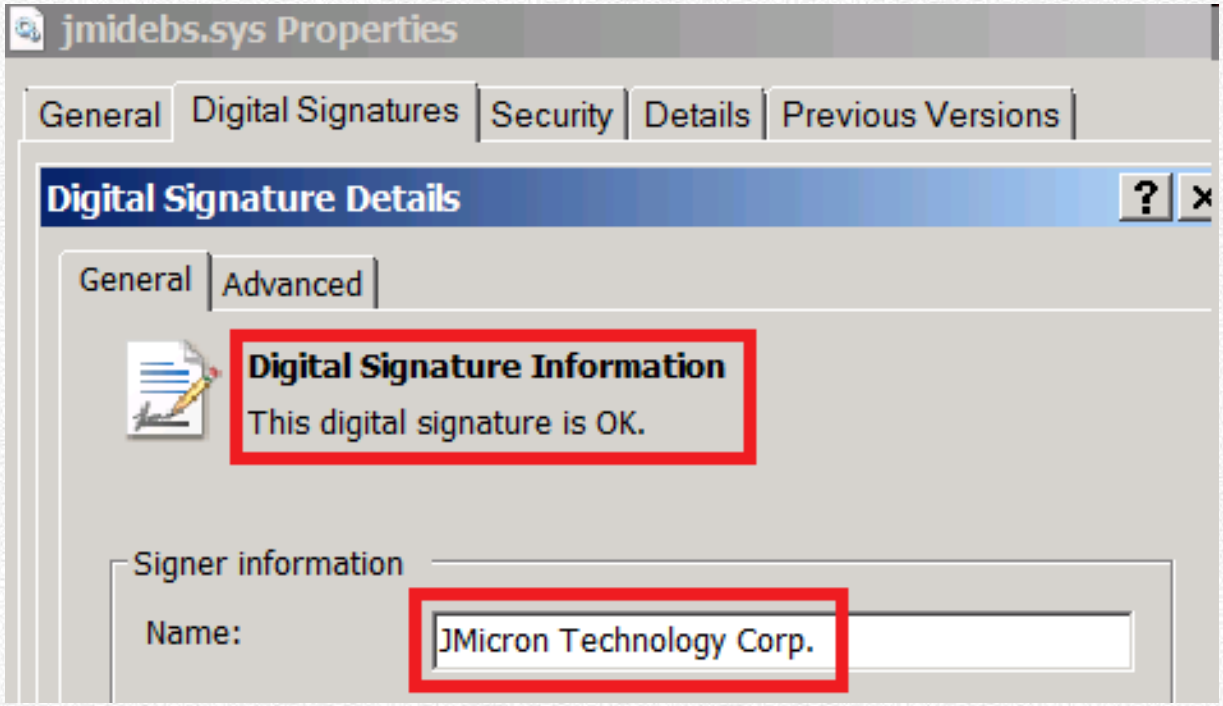
# Gestohlene Zertifikate



Stuxnet (enthielt Zertifikate für JMicron & Realtek)

Verwendet gestohlene Zertifikate

Entdeckt von ESET



Comodo Incident 2011:

*"Ich Sun broke into Comodo's Italian registration authority, called Comodo Italy, and on March 15 used Comodo's systems to fraudulently issue nine digital certificates."*

Stellt unter anderem zwei "Certificate Signing" Zertifikate aus.

# Hilft Extended Validation?



Extended Validation:

- Richtlinien von CA/Browser Forum (Ca. 30 bis 40 Mitglieder Oct 2009)
- Zielsetzungen:
  - "Identify the legal entity that controls a Web site"
  - "Enable encrypted communications with a Web site"
  - "Identify the source of executable code"
  - "The secondary purposes of an EV Certificate are to help establish the legitimacy of a business"
  - "addressing problems relatedto phishing, malware, and other forms of online identity fraud"

# EV Umsetzung:



Speziell OIDs z.B.:

- 1.3.6.1.4.1.6449.1.2.1.5.1 Comodo EV CPS

Browser zeigen zusätzliche Merkmale

- Stanford University 2006:
- "Extended validation did not help users defend against either attack"
- "Extended validation did not help untrained users classify a legitimate site"
- "Training caused more real and fraudulent sites to be classified as legitimate"

## This Connection is Untrusted

You have asked Firefox to connect securely to **portal.ktn.gv.at**, but we can't confirm that your connection is secure.

Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.

### What Should I Do?

If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.

Get me out of here!

- Technical Details
- I Understand the Risks

# Fazit digitale Zertifikate:

DEEPSEC

- Komplexe Technik
- Viele Mitspieler
- Nicht jeder ist vertrauenswürdig
- Anwender ist überfordert
- Umfangreiche Angriffsvektoren
- Incidents werden oft spät erkannt

# Internet Routing

# Routing Angriffe im Internet

DEEPSEC

- Internet ist ein Netz von Netzen
- Keinen Zentrale Registrierung, wer mit wem redet
- Falsche Routing Information denkbar:
  - Genauere Information bevorzugt
  - Z.B. “Berlin Charlottenburg” oder nur “Berlin”

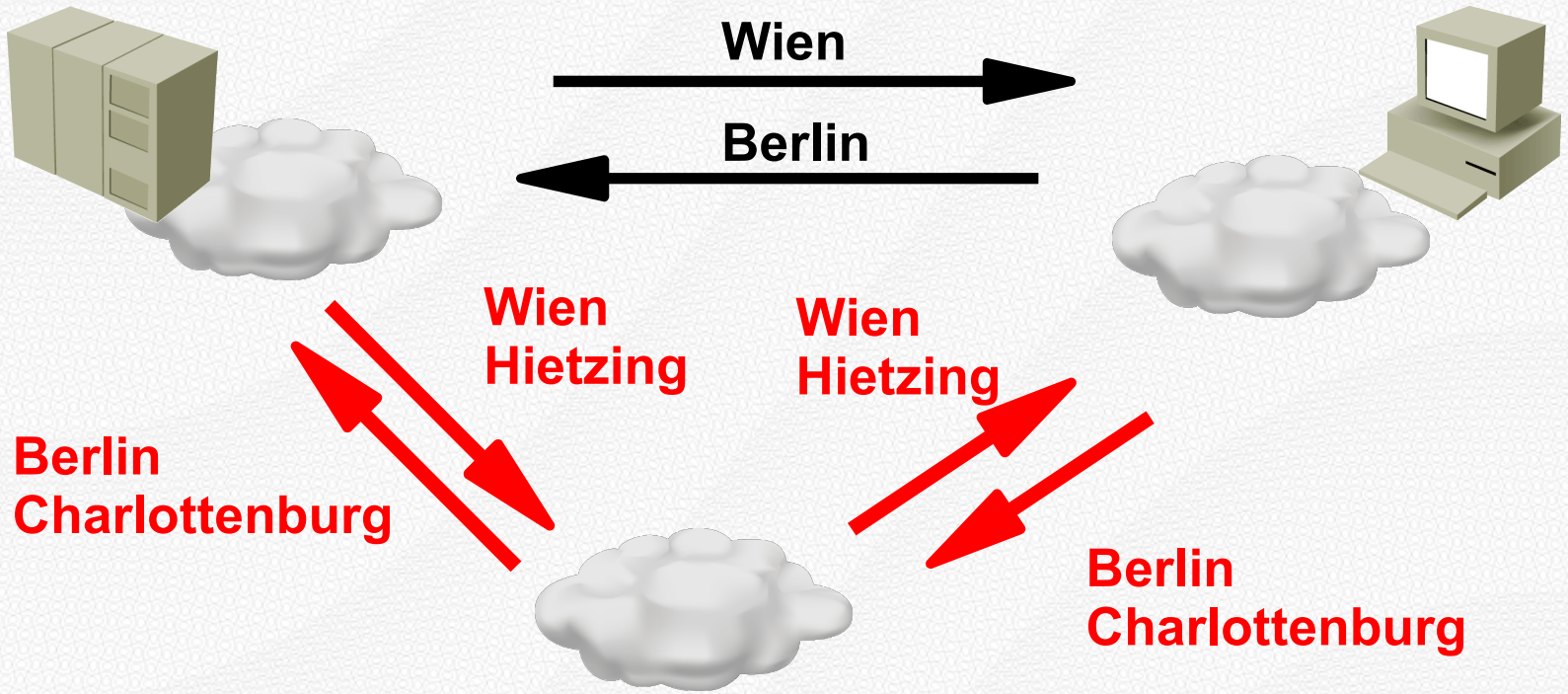
# Internet: Ein Netz von Netzen



- Vertrauen implizit
- Routing (weiterleiten von Daten) kann nicht verifiziert werden.
- Dynamisches verhalten.
- Falsche Routing Information kann eingeschleust werden (siehe folgende Seiten).
- Erkennung sehr schwer.

# Ein Routing Angriff





# Kombinierte Attacken

DEEPSEC

- Attacken treten selten einzeln auf
- Kombination
  - zur Ablenkung/Vortäuschung/Verwirrung
  - zur Übernahme von Systemen als Angriffsplattform
  - zum Attackieren mehrere Systemarten
- Einsatz kombinierter Schadsoftware

…as we know, there are known knowns. There are things we know we know. We also know there are known unknowns. That is to say we know there are some things we do not know. But there are also unknown unknowns -- the ones we don't know we don't know.
– *Donald Rumsfeld, 12.2.2002, Department of Defense news briefing*

# Über uns…

DEEPSEC

The DeepSec IDSC is an annual European two-day in-depth conference on computer, network, and application security. We aim to bring together the leading security experts from all over the world. DeepSec IDSC is a non-product, non-vendor-biased conference event. Intended target audience: Security Officers, Security Professionals and Product Vendors, IT Decision Makers, Policy Makers, Security-/Network-/Firewall-Admins, Hackers and Software Developers.

Web: https://deepsec.net/
Blog: http://blog.deepsec.net/