

An Overview of Cybercrime



Agenda

- Adversaries in Cyberspace
- Cybercrime
- Trends
- About DeepSec IDSC

Adversaries

Hackers

- Origins in 1970s
- Driven by curiosity & creativity
- Spreading after 2000
 - Social Hacking
 - Urban Hacking
 - Food Hacking
 - ...
- *Mostly harmless*

H4x0rS

- „Script Kiddies” - Internet as playground
- Fertile ground
 - Cheap hardware, easy access to software
 - Simple & „anonymous” communication
 - No ethics, little skills
- Higher risk, smaller impact
- Watch out for vacation periods!

Hacktivism

- *Here we come with zeal!*
- Motivation political or religious
- Ethics driven by urge to create awareness
- High risk potential


Hacktivist

Turkish Defacer Team - Turkish Defacer Team - Mozilla Firefox

Datei Bearbeiten Ansicht Chronik Lesezeichen Extras Hilfe

Disable Cookies CSS Forms Images Information Miscellaneous Outline Resize Tools View Source Options

Proxy: Apply Edit Remove Add Status: Preferences



Turkish Defacer Team

Kullanıcı ismi Beni hatırla
Şifreniz

Turkish Defacer Team 'una Hoşgeldiniz.

Bu Forumu yaptığınız ilk ziyaretiniz ise, Lütfen öncelikle **Yardım** kriterlerini okuyun. Forumda bilgi alışverişinde bulunabilmemiz için öncelikle **Kayıt** olmalısınız. Üye olmayanlar forumda hiçbir şekilde aktivite uygulayamaz, Mesaj yazamaz, Konu açamaz, konu okuyamaz, program indiremez. Forum'u tam anlamıyla kullanabilmek için Üyelik şarttır ve ücretsizdir.

TDT Yönetim

Warez Hosting

Forum	son Mesaj	Konular	Mesajlar	Moderatörler
Warez Hosting Paketleri Warez hosting paket detaylarını buradan inceleyebilirsiniz <ul style="list-style-type: none">WStandart (1/1)WBronz (1/1)WGold (1/1)	WGold - Warez Gold Paket yazan badcat 05-07-2007 01:02 AM	3	3	

Duyurular

Fertig

Hacktivists



xv_x@live.com

dr.ze3la

MoRoCcaN HaCkEr

Ethical Hacking

- „White Hats”
- Professional hacking
 - Penetration tests
 - Verification of integrity and defences
 - Responsible reporting
- Effort to improve public opinion of hacking
- No risks, no impact

Cybercrime

Cybercrime?

Computer crime can broadly be defined as criminal activity involving an information technology infrastructure, including illegal access (unauthorized access), illegal interception (by technical means of non-public transmissions of computer data to, from or within a computer system), data interference (unauthorized damaging, deletion, deterioration, alteration or suppression of computer data), systems interference (interfering with the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data), misuse of devices, forgery (ID theft), and electronic fraud.

-- [Wikipedia: Computer Crime](#)

Phishing & Scams

- Exploit messaging channels
- Mimicking of original web sites
- Scams
 - Charity, bomb threat, lottery, fake offers, ...
- Trick victims into
 - leaking information
 - signing contracts (buying things)
 - act as a messenger

Phishing Sample



[Sign Up](#) | [Log In](#) | [Help](#) | [Security Center](#)

Welcome

Send Money

Request Money

Merchant Tools

Auction Tools

Member Log-In

Email Address

Password

Log In

[Forgot your email address?](#)
[Forgot your password?](#)

Join PayPal Today

Now Over
100 million accounts

[Sign Up Now!](#)



Learn more about
[PayPal Worldwide](#)

Shop Without Sharing
Your Financial Information

PayPal. Privacy is built in. [Learn more](#)

Send money
NOT your financial info

[Watch how PayPal works](#)



PayPal Mobile

[Learn more](#)

Buyers

[Send money](#) with an email address in 103 countries and regions.

PayPal is [free for buyers](#).

Shop without sharing [financial information](#).

[100% protection](#) against unauthorized payments sent from your account.

eBay Sellers

[Free eBay tools](#) make selling easier.

PayPal works hard to help [protect sellers](#).

PayPal simplifies [shipping and tracking](#).

[Earn cash back](#) with PayPal Preferred Rewards.

Merchants

[Accept credit cards online](#) with PayPal.

Get paid by phone, fax, and mail with [Virtual Terminal](#).

See how PayPal can [increase your sales](#).

Learn more about our secure [Merchant Services](#).

[Compare our solutions side by side](#).

What's New

[Visit the Online Merchant Network](#)

[Big Brands Accepting PayPal](#)

Special Offers

[16 Ways to Grow Your E-Business](#)

[Free Alerts to Help Protect You From ID Theft](#)

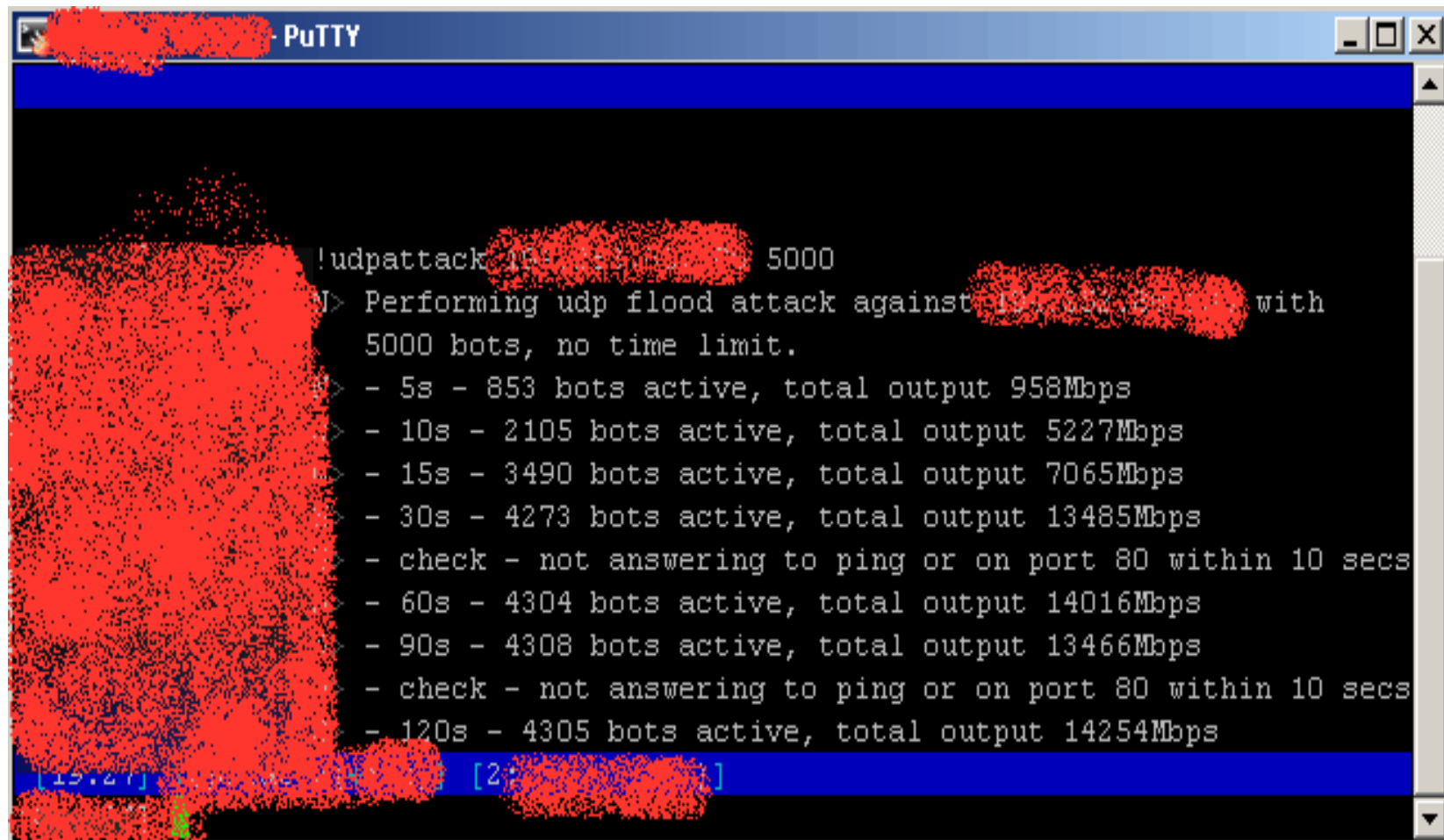
Social Engineering

- Exploits *cognitive bias*
- Pretexting, baiting, (phone) phishing, ...
- Can be done by any network or by proxy
- Can circumvent *any* technology
- Low-tech attack, high impact

Bot Herding

- Modern cowboys herd robots
 - Bots live on infected machines (*zombies*)
 - Bots connect by Command & Control (C&C) network
- Rent network and computing power for
 - Sending spams
 - Brute-forcing / flooding services
 - Proxying attacks
 - Logging keystrokes
- Cost per PC \cong \$1 or less
- Cloud Computing for criminals

DDoS Bot Attack



```
!udpattack [redacted] 5000
> Performing udp flood attack against [redacted] with
  5000 bots, no time limit.
> - 5s - 853 bots active, total output 958Mbps
> - 10s - 2105 bots active, total output 5227Mbps
> - 15s - 3490 bots active, total output 7065Mbps
> - 30s - 4273 bots active, total output 13485Mbps
> - check - not answering to ping or on port 80 within 10 secs
> - 60s - 4304 bots active, total output 14016Mbps
> - 90s - 4308 bots active, total output 13466Mbps
> - check - not answering to ping or on port 80 within 10 secs
> - 120s - 4305 bots active, total output 14254Mbps
```


Botnet C&C

```
mIRC [356983] [+CmMnstu]
File View Favorites Tools Commands Window Help
* [2K3|USA]50507145 has joined
* [XP|USA]88899812 has joined
* [2K|USA]19369043 has quit IRC (Connection reset by peer)
* [XP|USA]34398706 has joined
* [2K|USA]05035720 has joined
* [2K|USA]58505503 has quit IRC (Connection reset by peer)
* [2K|USA]97293378 has quit IRC (Connection reset by peer)
* [XP|USA]71057940 has joined
* [XP|USA]62263862 has quit IRC (Connection reset by peer)
* [2K|USA]93901567 has quit IRC (Connection reset by peer)
* [XP|USA]29125843 has quit IRC (Connection reset by peer)
* [XP|USA]73625442 has joined
* [XP|USA]93108059 has joined
* [XP|USA]25502583 has quit IRC (Connection reset by peer)
* [XP|USA]37774925 has quit IRC (Connection reset by peer)
* [XP|USA]19712721 has quit IRC (Connection reset by peer)
* [2K|USA]23808428 has quit IRC (Connection reset by peer)
* [2K|USA]37194548 has quit IRC (Connection reset by peer)
* [2K|USA]12091301 has quit IRC (Connection reset by peer)
* [XP|USA]67876432 has joined
* [2K|USA]13888067 has quit IRC (Connection reset by peer)
* [XP|USA]15106072 has quit IRC (Connection reset by peer)
* [2K3|USA]46287846 has joined
* [2K|USA]56377502 has joined
* [2K|USA]70798176 has joined
* [2K|USA]36697646 has joined
* [2K|USA]35325721 has quit IRC (Connection reset by peer)
* [XP|USA]79053641 has quit IRC (Connection reset by peer)
* [2K|USA]31600906 has joined
* [2K|USA]31896371 has joined
* [2K|USA]26348182 has joined
* [XP|USA]80331747 has joined
* [XP|USA]08391724 has quit IRC (Connection reset by peer)
* [2K|USA]93435010 has joined
* [2K|USA]83171118 has joined
* [2K|USA]07713611 has quit IRC (Connection reset by peer)
* [2K|USA]35401458 has quit IRC (Connection reset by peer)
* [2K|USA]44354555 has joined
* [2K|USA]21029524 has quit IRC (Connection reset by peer)
[2K3|USA]46541351
[2K3|USA]32605043
[2K3|USA]00225565
[2K3|USA]00787465
[2K3|USA]01035702
[2K3|USA]01265285
[2K3|USA]02333711
[2K3|USA]02927631
[2K3|USA]03638723
[2K3|USA]04395318
[2K3|USA]06507555
[2K3|USA]07917517
[2K3|USA]08374933
[2K3|USA]09913893
[2K3|USA]10177973
[2K3|USA]10325689
[2K3|USA]10843550
[2K3|USA]11176395
[2K3|USA]11251967
[2K3|USA]11692505
[2K3|USA]12406645
[2K3|USA]12608295
[2K3|USA]13938417
[2K3|USA]14128258
[2K3|USA]14524213
[2K3|USA]14878082
[2K3|USA]14956279
[2K3|USA]14985134
[2K3|USA]15026298
[2K3|USA]15189717
[2K3|USA]15217466
[2K3|USA]15845049
[2K3|USA]16363078
[2K3|USA]16960314
[2K3|USA]16966148
[2K3|USA]17440107
[2K3|USA]17453764
[2K3|USA]17973773
```

Sophisticated Botnets

- Modern Botnets
 - use encrypted channels for C&C
 - can be upgraded with payloads
 - automatically collect logins, passwords, ...
 - use hard-to-detect software agents
- Tool of Cyber Warfare and Organised Crime

Online Markets

- Stolen goods / services are traded on markets
 - Credit cards, logins for bank accounts
 - Identities, digital copies of passports
 - Access to Botnets
 - Virtual currencies (World of Warcraft gold, ...)
- Anonymity not desirable – think reputation
- Trade is done by escrow
 - Trusted third party used for deal
 - Escrow may inspect payment / goods

Pricing - Examples

- UK bank account details - £5
- 50 credit card numbers - £20
- 1.000 infected PCs
 - Australian PCs - \$100
 - PCs in the Far East/other countries - \$5
- Identity sets - \$2 each (\$30 per EU identity)
 - Social security number, name, address, date of birth

Industrial Espionage

- Information determines the future of your company
- Highly specialised attacks
- Well funded
 - backed by governments
 - backed by large corporations
- Not very common, high risk, high impact

Industrial-Espionage.cn

„...In the months leading up to the 2007 operation, cyberspies did extensive reconnaissance, identifying which employee computer accounts they wanted to hijack and which files they wanted to steal. They obtained credentials for dozens of employee accounts, which they accessed nearly 150 times....The hackers copied and transferred files to seven servers hosting the company's email system, which were capable of processing large amounts of data quickly. Once they moved the data to the email servers, the intruders renamed the stolen files to blend in with the other files on the system and compressed and encrypted the files for export.”

-- [China Expands Cyberspying in U.S., Report Says](#), Wall Street Journal

„...The attackers used at least eight US-based computers, some at universities, as drop boxes before sending it overseas. The company's security team managed to detect the theft while it was in progress, but not before significant amounts of data left the company network....”

-- [China fingered in cyberattack on mystery high tech co.](#), The Register®

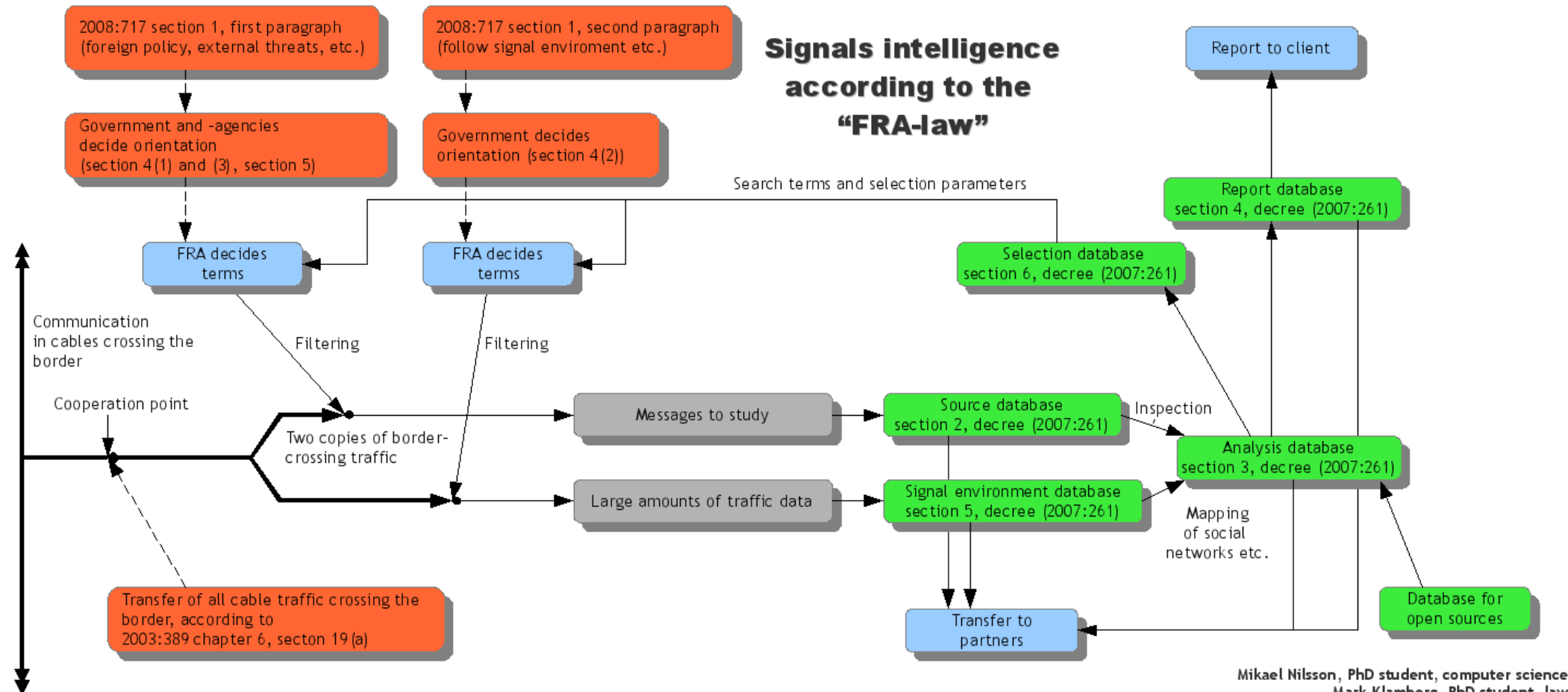
Industrial-Espionage.gov

Why, then, have we spied on you? The answer is quite apparent from the Campbell report – in the discussion of the only two cases in which European companies have allegedly been targets of American secret intelligence collection. Of Thomson-CSF, the report says: „The company was alleged to have bribed members of the Brazilian government selection panel.” Of Airbus, it says that we found that „Airbus agents were offering bribes to a Saudi official.” These facts are inevitably left out of European press reports.

That’s right, my continental friends, we have spied on you because you bribe. Your companies’ products are often more costly, less technically advanced or both, than your American competitors’. As a result you bribe a lot. So complicit are your governments that in several European countries bribes still are tax-deductible.

-- [R. James Woolsey](#), a Washington lawyer and a former Director of Central Intelligence., The Wall Street Journal, March 17, 2000.

Industrial-Espionage.se



Mikael Nilsson, PhD student, computer science
Mark Klamberg, PhD student, law
Anna Petersson, PhD student, mathematics

<http://stoppaFRAlagen.nu>
<http://klamberg.blogspot.com>

Trends

- Botnets, Zombies and Trojan Horses
- Social Engineering
- Mobile devices / computing
- Shadow economy keeps booming

Questions?



DeepSec IDSC

The [DeepSec IDSC](#) is an annual European two-day in-depth conference on computer, network, and application security. The mission statement is to bring together the world's most renowned security professionals from academics, government, industry, and the underground hacking community. DeepSec aims to be a strictly neutral platform and a meeting point for everyone involved in security.

Contact: Michael Kafka & René Pfeiffer, deepsec@deepsec.net

Copyright Information

- Some rights reserved. / Einige Rechte vorbehalten.
- [DeepSec GmbH](#), Vienna, Austria.
- You may freely use, distribute and modify this work under the following agreement:
 - Authors must be referenced (also for modification) / Autoren müssen genannt werden (auch bei Bearbeitung)
 - Only for non-commercial use / nur für nichtkommerzielle Nutzung
 - Derivative work under the same license / Derivative Arbeit unter derselben Lizenz



An Overview of Cybercrime



This presentation tries to inform about „cybercriminal” activities throughout the Internet and related communication channels. Examples are given, albeit the talk can only be a broad overview. Studies in greater details are scarce, only security companies and some law enforcement agencies have published papers.

The cover page shows a graffiti found on a wall in Vienna, Austria.

Agenda

- Adversaries in Cyberspace
- Cybercrime
- Trends
- About DeepSec IDSC

Adversaries

It's always good to know who the opponents are and what their motivation is.

Hackers

- Origins in 1970s
- Driven by curiosity & creativity
- Spreading after 2000
 - Social Hacking
 - Urban Hacking
 - Food Hacking
 - ...
- *Mostly harmless*

4

DeepSec IDSC

[John T. Draper](#), also known as *Captain Crunch*, *Crunch* or *Crunchman*, is an example of early hacking. [Phreaking](#) was the first playground of hackers. It involves the exploitation of [in-band signaling](#) used in telephone lines. By injecting a 2600 Hz tone the phone system one could gain operator status and use the network to reroute or place calls. Today's hackers have a similar approach to technology. The term hacking generally refers to discovering how a device, software, hardware or protocol works and to use this knowledge in order to create modifications. Hacking can be done with hardware, software, legal codes, musical instruments (preferably electronic ones), electronic devices and more. One's own creativity is the limit.

H4x0rS

- „Script Kiddies” - Internet as playground
- Fertile ground
 - Cheap hardware, easy access to software
 - Simple & „anonymous” communication
 - No ethics, little skills
- Higher risk, smaller impact
- Watch out for vacation periods!

The terms *script kiddie*, or *skiddie*, occasionally *script bunny*, *skid*, *script kitty*, *script-running juvenile* (SRJ), or similar, are used for juveniles who lack the ability to create sophisticated code (or even any code) on their own. Instead they rely on tools they find and use them to impress their friends or peers. The tools they used often include password stealers, mass emailers, denial-of-service software, automatic scanners/crackers, and the like.

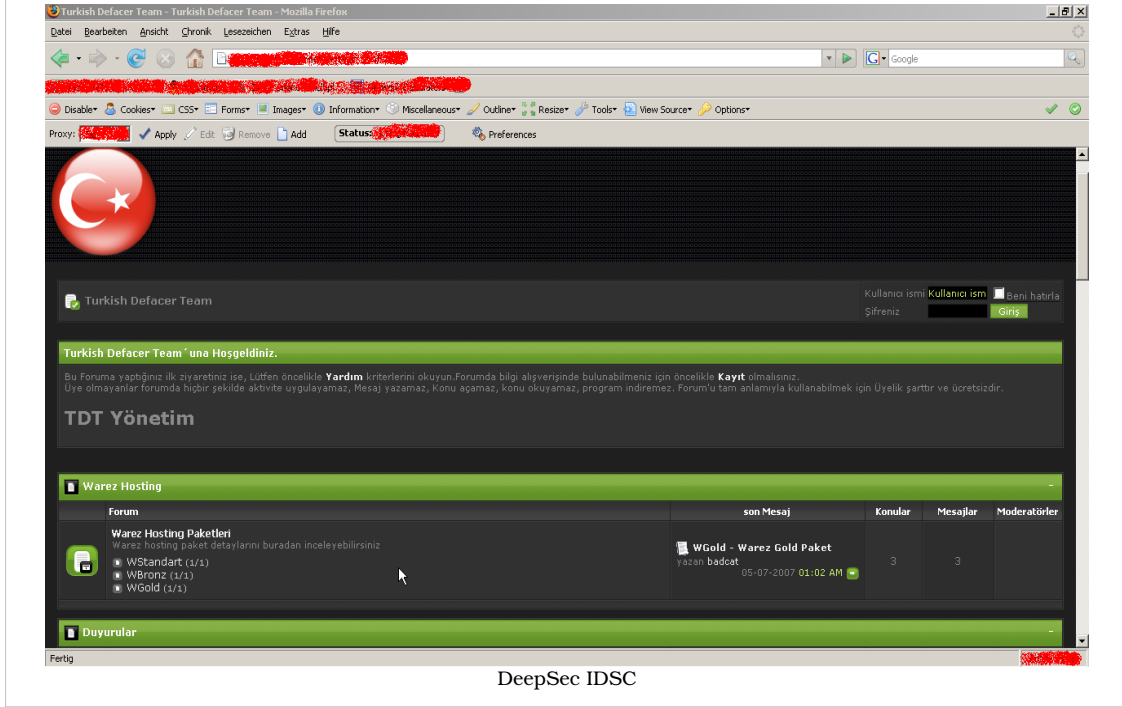
Hacktivism

- *Here we come with zeal!*
- Motivation political or religious
- Ethics driven by urge to create awareness
- High risk potential

Hacktivism has a cause. The term is derived from *hack* and *activist*. Their cause is mostly of political or religious flavour. Their actions range from peaceful protests to malicious cyber-attacks, depending on personal ethics. They can be a risk for network infrastructure, and their actions may be exploited by others for their own purposes (for example criminals might exploit attacks by hacktivists for their own goals). Most attacks are targeted at public web sites (i.e. by defacements) or the reputation of their opponents.

Incidents are often coupled to events, so some security administrators also screen news channels and press releases in order to gauge and predict incoming attacks.

Hacktivists



The screen shot shows a typical web site defacement. In this case it was done by a group of Turkish hacktivists.

Hacktivism



8

DeepSec IDSC

The screen shot shows a relatively new defacement performed by a Moroccan hacktivist. In this case the attack was carried out by automated tools, leading to a mass defacement of hundreds of web sites. The impact was low since the tools only replace the index page of the web space.

Ethical Hacking

- „White Hats”
- Professional hacking
 - Penetration tests
 - Verification of integrity and defences
 - Responsible reporting
- Effort to improve public opinion of hacking
- No risks, no impact

Ethical hacking refers to the use of one's hacking skills for „good” causes. Usually the term describes the use of hacking skills as a service provider. This implies adhering to strict rules and staying within the limits of the law. Ethical hackers perform tests of security systems by using the same tools and tactics attackers would use. The tests are recorded and the results, together with a risk assessment, is given to the customer.

Cybercrime

The term cybercrime is often used as a catch-all word for anything illegal, malicious or simply not well understood. Law enforcement usually denotes illegal acts of information security with this term. In politics the word is a lot less well-defined. This is a problem in many discussions where representatives of distinct groups take part. The following chapter tries to shed some light on the meaning of cybercrime. Our interpretation is similar to the one used by law enforcement. The

[description from Wikipedia](#) is a good start, too:

Computer crime can broadly be defined as criminal activity involving an information technology infrastructure, including illegal access (unauthorized access), illegal interception (by technical means of non-public transmissions of computer data to, from or within a computer system), data interference (unauthorized damaging, deletion, deterioration, alteration or suppression of computer data), systems interference (interfering with the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data), misuse of devices, forgery (ID theft), and electronic fraud.

Cybercrime?

Computer crime can broadly be defined as criminal activity involving an information technology infrastructure, including illegal access (unauthorized access), illegal interception (by technical means of non-public transmissions of computer data to, from or within a computer system), data interference (unauthorized damaging, deletion, deterioration, alteration or suppression of computer data), systems interference (interfering with the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data), misuse of devices, forgery (ID theft), and electronic fraud.

-- [Wikipedia: Computer Crime](#)

11

DeepSec IDSC

This is simply a quote from the English Wikipedia site. It is **not** a law nor a complete definition.

Phishing & Scams

- Exploit messaging channels
- Mimicking of original web sites
- Scams
 - Charity, bomb threat, lottery, fake offers, ...
- Trick victims into
 - leaking information
 - signing contracts (buying things)
 - act as a messenger

12

DeepSec IDSC

Phishing and scams usually use advantage of unsolicited bulk email (UBE) or unsolicited commercial email (UCE), also known as *spam*. Other communications channels such as fax or old-fashioned mail is also used. Users are tricked into visiting a web site and leaving personal information. This information is harvested and sold. Some multi-stage scams include contacting the user with false promises and more information designed to trick the user into doing more actions.

The famous [Nigerian Scam](#) has its origins in the early 1980s, trying to manipulate business visitors interested in shady deals in the Nigerian oil sector. The schema has expanded to other countries and countless of variations.

Phishing Sample



[Sign Up](#) | [Log In](#) | [Help](#) | [Security Center](#)

[Welcome](#) | [Send Money](#) | [Request Money](#) | [Merchant Tools](#) | [Auction Tools](#)

Member Log-In	Forgot your email address? Forgot your password?	Join PayPal Today Now Over 100 million accounts Sign Up Now!	Learn more about PayPal Worldwide
Email Address <input type="text"/>			
Password <input type="password"/>	<input type="button" value="Log In"/>		



Send money
NOT your financial info

[Watch how PayPal works](#)

PayPal Mobile
[Learn more](#)

Buyers

[Send money](#) with an email address in 103 countries and regions.

PayPal is [free for buyers](#).

Shop without sharing [financial information](#).

[100% protection](#) against unauthorized payments sent from your account.

eBay Sellers

[Free eBay tools](#) make selling easier.

PayPal works hard to help [protect sellers](#).

PayPal simplifies [shipping and tracking](#).

[Earn cash back](#) with PayPal Preferred Rewards.

Merchants

[Accept credit cards online](#) with PayPal.

Get paid by phone, fax, and mail with [Virtual Terminal](#).

See how PayPal can [increase your sales](#).

Learn more about our secure [Merchant Services](#).

[Compare our solutions side by side](#).

What's New

[Visit the Online Merchant Network](#)

[Big Brands Accepting PayPal](#)

Special Offers

[16 Ways to Grow Your E-Business](#)

[Free Alerts to Help Protect You From ID Theft](#)

[About](#) | [Accounts](#) | [Fees](#) | [Privacy](#) | [Security Center](#) | [Contact Us](#) | [Legal Agreements](#) | [Developers](#) | [Jobs](#) | [Mobile](#) | [Plus Card](#) | [Referrals](#) | [Shops](#) | [Mass Pay](#)

This is not the real PayPal.com web site.

Social Engineering

- Exploits *cognitive bias*
- Pretexting, baiting, (phone) phishing, ...
- Can be done by any network or by proxy
- Can circumvent *any* technology
- Low-tech attack, high impact

Cognitive Bias: *A cognitive bias is a person's tendency to make errors in judgment based on cognitive factors, and is a phenomenon studied in cognitive science and social psychology. Forms of cognitive bias include errors in statistical judgment, social attribution, and memory that are common to all human beings. Such biases drastically skew the reliability of anecdotal and legal evidence. These are thought to be based upon heuristics, or rules of thumb, which people employ out of habit or evolutionary necessity.*

Humans are the weakest link in the chain of security measures.

Bot Herding

- Modern cowboys herd robots
 - Bots live on infected machines (*zombies*)
 - Bots connect by Command & Control (C&C) network
- Rent network and computing power for
 - Sending spams
 - Brute-forcing / flooding services
 - Proxying attacks
 - Logging keystrokes
- Cost per PC \cong \$1 or less
- Cloud Computing for criminals

15

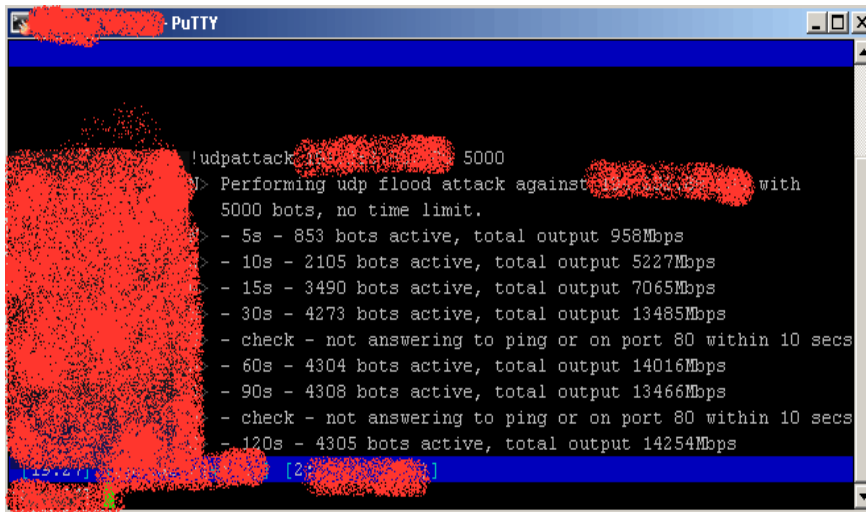
DeepSec IDSC

Botnets have become the ultimate tool for online crime. A robot or bot is an infected computer connected to the Internet. Cheap Internet connections and energy prices have led to „always on” computers. Compromised machines connect to a Command & Control network and receive their orders from the Botnet commanders or from customers who have rented the Botnet or parts of it.

The [size of Botnets](#) range from approximately a few thousand to several million computers. The exact sizes are not known. The penetration of infected machines goes beyond perimeter defences, thus Botnets penetrate even well-known organisations and companies (such as French Navy, Bundeswehr, UK Ministry of Defence).

Infection of clients is done by web browser vulnerabilities (drive-by downloads), worms, Trojan horses, viruses or other malicious software.

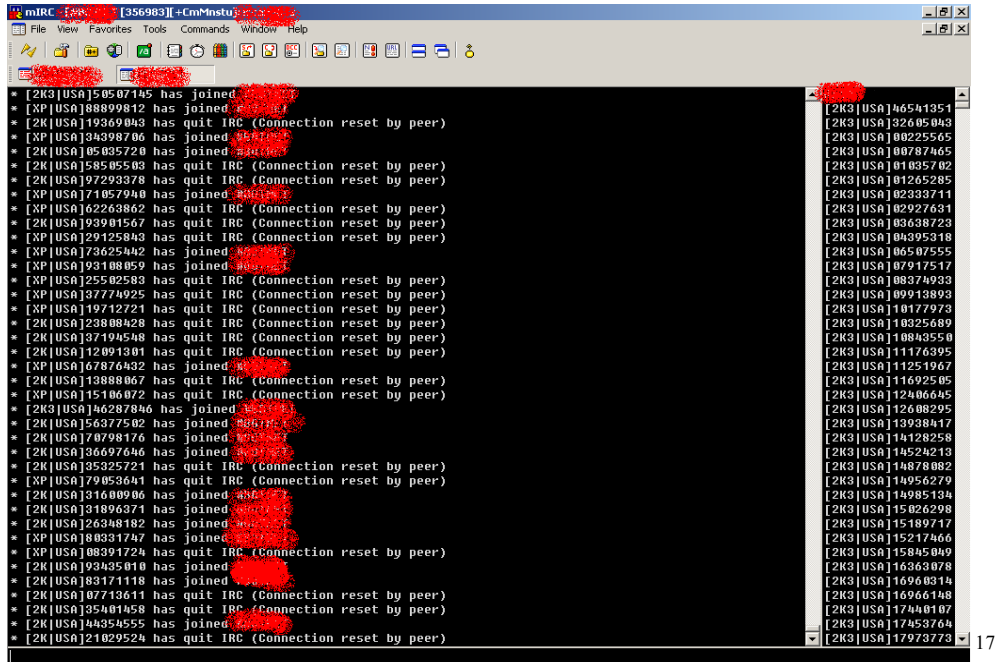
DDoS Bot Attack



```
udppattack -s 192.168.1.100 -d 192.168.1.1 -p 80 -c 5000
> Performing udp flood attack against 192.168.1.1 with
5000 bots, no time limit.
> - 5s - 853 bots active, total output 958Mbps
> - 10s - 2105 bots active, total output 5227Mbps
> - 15s - 3490 bots active, total output 7065Mbps
> - 30s - 4273 bots active, total output 13485Mbps
> - check - not answering to ping or on port 80 within 10 secs
> - 60s - 4304 bots active, total output 14016Mbps
> - 90s - 4308 bots active, total output 13466Mbps
> - check - not answering to ping or on port 80 within 10 secs
> - 120s - 4305 bots active, total output 14254Mbps
```

The screen shot shows a small Botnet at work. 5000 clients flood a target with UDP packets.

Botnet C&C



The screenshot shows a Windows-style IRC client window titled "mIRC [356983] [+CmMstu]". The main chat area displays a continuous stream of messages from various bots, including join and quit notifications. The messages are partially obscured by redacted areas. A scrollable list of bot identifiers is visible on the right side of the window, showing a range of IP addresses from [2K3|USA]46541351 to [2K3|USA]11793773. The window's taskbar and menu bar are also visible.

```
* [2K3|USA]150507145 has joined  
* [XP|USA]188809812 has joined  
* [2K|USA]19369043 has quit IRC (Connection reset by peer)  
* [XP|USA]348398706 has joined  
* [2K|USA]05005720 has joined  
* [2K|USA]58505503 has quit IRC (Connection reset by peer)  
* [2K|USA]97293378 has quit IRC (Connection reset by peer)  
* [XP|USA]71057940 has joined  
* [XP|USA]62263862 has quit IRC (Connection reset by peer)  
* [2K|USA]193901567 has quit IRC (Connection reset by peer)  
* [XP|USA]120125843 has quit IRC (Connection reset by peer)  
* [XP|USA]73625442 has joined  
* [XP|USA]93108059 has joined  
* [XP|USA]25502583 has quit IRC (Connection reset by peer)  
* [XP|USA]37774925 has quit IRC (Connection reset by peer)  
* [XP|USA]19712721 has quit IRC (Connection reset by peer)  
* [2K|USA]23808428 has quit IRC (Connection reset by peer)  
* [2K|USA]37194548 has quit IRC (Connection reset by peer)  
* [2K|USA]12091301 has quit IRC (Connection reset by peer)  
* [XP|USA]167876432 has joined  
* [2K|USA]18888067 has quit IRC (Connection reset by peer)  
* [XP|USA]15106072 has quit IRC (Connection reset by peer)  
* [2K3|USA]46287846 has joined  
* [2K|USA]56377502 has joined  
* [2K|USA]70798176 has joined  
* [2K|USA]36697646 has joined  
* [2K|USA]35325721 has quit IRC (Connection reset by peer)  
* [XP|USA]79053641 has quit IRC (Connection reset by peer)  
* [2K|USA]131600986 has joined  
* [2K|USA]31896371 has joined  
* [2K|USA]26348182 has joined  
* [XP|USA]80831747 has joined  
* [XP|USA]08391724 has quit IRC (Connection reset by peer)  
* [2K|USA]93435010 has joined  
* [2K|USA]83171118 has joined  
* [2K|USA]07713611 has quit IRC (Connection reset by peer)  
* [2K|USA]35701058 has quit IRC (Connection reset by peer)  
* [2K|USA]44345555 has joined  
* [2K|USA]21029524 has quit IRC (Connection reset by peer)
```

DeepSec IDSC

The screen shot shows a Botnet C&C channel. Infected machines connect to an IRC server. The commands are give on the C&C channel or individually to single bots or groups. Some Botnets have a sophisticated C&C software that can issue commands with a few mouse clicks. These tools can even be used for reconnaissance and passive attacks such as logging keystrokes or intercepting login credentials.

Sophisticated Botnets

- Modern Botnets
 - use encrypted channels for C&C
 - can be upgraded with payloads
 - automatically collect logins, passwords, ...
 - use hard-to-detect software agents
- Tool of Cyber Warfare and Organised Crime

The [Conficker Botnet](#) is a good example of a modern Botnet. It uses code that features automatic download of payloads, self-defence, encryption, digital certificates and automatic patches. Additionally Conficker disables certain Microsoft Windows services such as Automatic Updates, Background Intelligent Transfer Service (BITS), Windows Defender and Windows Error Reporting. The Conficker Botnet is the largest Botnet ever detected, and security researchers still have open questions about its purpose and the creators.

Online Markets

- Stolen goods / services are traded on markets
 - Credit cards, logins for bank accounts
 - Identities, digital copies of passports
 - Access to Botnets
 - Virtual currencies (World of Warcraft gold, ...)
- Anonymity not desirable – think reputation
- Trade is done by escrow
 - Trusted third party used for deal
 - Escrow may inspect payment / goods

19

DeepSec IDSC

This is the most interesting aspect of cybercrime – the economical side. Wherever there's demand, markets will grow. By offering stolen digital goods new organised crime syndicates have come into existence. One notable group was [ShadowCrew](#):

ShadowCrew was an international crime message board that offered a haven for carders or "hackers" to trade, buy, and sell anything from stolen personal information, to hacked credit card numbers and false identification. Shadowcrew emerged from another underground site, counterfeitlibrary.com in early 2002 and would be followed up by carderplanet.com, a primarily Russian site.

ShadowCrew was attacked by the US Secret Service, the FBI and several police departments from around the world. 28 members of ShadowCrew were raided and arrested after monitoring their activities for over a year (Operation Firewall). According to an article in the [ISSA Journal](#) (issue October 2005) the law enforcement staff found 1.7 million stolen credit card numbers and account information for 18 million emails accounts.

Pricing - Examples

- UK bank account details - £5
- 50 credit card numbers - £20
- 1.000 infected PCs
 - Australian PCs - \$100
 - PCs in the Far East/other countries - \$5
- Identity sets - \$2 each (\$30 per EU identity)
 - Social security number, name, address, date of birth

Prices vary depending on the quality of the goods. Identity vary by country.

Industrial Espionage

- Information determines the future of your company
- Highly specialised attacks
- Well funded
 - backed by governments
 - backed by large corporations
- Not very common, high risk, high impact

Albeit the term industrial or corporate espionage suggests that only the commercial sector is involved, this is not the whole truth. Intelligence services protect national interests, and if commercial success is in the interest of the nation, then these departments are players, too. Countering attacks on this level is very hard, because few organisations can muster the resources to do so.

Industrial-Espionage.cn

„...In the months leading up to the 2007 operation, cyberspies did extensive reconnaissance, identifying which employee computer accounts they wanted to hijack and which files they wanted to steal. They obtained credentials for dozens of employee accounts, which they accessed nearly 150 times....The hackers copied and transferred files to seven servers hosting the company's email system, which were capable of processing large amounts of data quickly. Once they moved the data to the email servers, the intruders renamed the stolen files to blend in with the other files on the system and compressed and encrypted the files for export.”

-- [China Expands Cyberspying in U.S., Report Says](#), Wall Street Journal

„...The attackers used at least eight US-based computers, some at universities, as drop boxes before sending it overseas. The company's security team managed to detect the theft while it was in progress, but not before significant amounts of data left the company network...”

-- [China fingered in cyberattack on mystery high tech co.](#), The Register®

23

DeepSec IDSC

These two news items were published very recently.

Industrial-Espionage.gov

Why, then, have we spied on you? The answer is quite apparent from the Campbell report – in the discussion of the only two cases in which European companies have allegedly been targets of American secret intelligence collection. Of Thomson-CSF, the report says: „The company was alleged to have bribed members of the Brazilian government selection panel.” Of Airbus, it says that we found that „Airbus agents were offering bribes to a Saudi official.” These facts are inevitably left out of European press reports.

That’s right, my continental friends, we have spied on you because you bribe. Your companies’ products are often more costly, less technically advanced or both, than your American competitors’. As a result you bribe a lot. So complicit are your governments that in several European countries bribes still are tax-deductible.

-- [R. James Woolsey](#), a Washington lawyer and a former Director of Central Intelligence., The Wall Street Journal, March 17, 2000.

24

DeepSec IDSC

This text is an excerpt from an article published in the Wall Street Journal. Mr. Woolsey was as former Director of Central Intelligence and head of the Central Intelligence Agency (February 5, 1993 - January 10, 1995). His article is a riposte on the [Echelon](#) discussion in Europe. He defends spying on European businesses as an act of self-defence against bribery and the invasion of „inferior” European technology.

The article clearly illustrates the connection between government intelligence agencies and the commercial sector.

Trends

- Botnets, Zombies and Trojan Horses
- Social Engineering
- Mobile devices / computing
- Shadow economy keeps booming

It's always very difficult to predict developments in computer security. However botnets have proven to be very versatile and useful tools for attackers. Consider the Conficker botnet and its world-wide penetration. Infecting local computers from networks is done frequently (especially web browser bugs in combination with errors in browser plug-ins/add-ons ensure this attack vector). Social engineering is part of every scam and phishing attack. This means that creating security awareness among users is a prime goal of every security effort. Few really know what consequences their actions can have.

Given the financial impact of shadow markets their continuing existence is certain. The global financial crisis is also a major motivator for turning to alternative sources of revenue and selling stolen information (such as technology or accounts that can be used for attacks).

Questions?



DeepSec IDSC

The [DeepSec IDSC](#) is an annual European two-day in-depth conference on computer, network, and application security. The mission statement is to bring together the world's most renowned security professionals from academics, government, industry, and the underground hacking community. DeepSec aims to be a strictly neutral platform and a meeting point for everyone involved in security.

Contact: Michael Kafka & René Pfeiffer, deepsec@deepsec.net

Copyright Information

- Some rights reserved. / Einige Rechte vorbehalten.
- [DeepSec GmbH](#), Vienna, Austria.
- You may freely use, distribute and modify this work under the following agreement:
 - Authors must be referenced (also for modification) / Autoren müssen genannt werden (auch bei Bearbeitung)
 - Only for non-commercial use / nur für nichtkommerzielle Nutzung
 - Derivative work under the same license / Derivative Arbeit unter derselben Lizenz

