

## 16TH IAP EUROPEAN REGIONAL CONFERENCE

### NEW INVESTIGATIVE APPROACHES TO TACKLE CRIMINAL ORGANIZATIONS USING THE INTERNET

Tirana 22-24 May 2017



# Cybercrime – phenomena, prosecution and challenges

Cai Rueffer, Public Prosecutor

Office of the Attorney General of the Federal State of Hesse – Cybercrime-Center



# Agenda

## Part 1

### Introduction of the Cybercrime-Center

- Tasks, responsibility, features ...

## Part 2

### Cases being dealt with

- Cybercrime and „Underground Economy“
- Darknet and illicit goods being trafficked
- Child pornography and „crime as a service“

## Part 3

### Investigation methods and challenges

- Investigations – our tools, methods and experiences
- Encryption, Anonymization, Internationalization



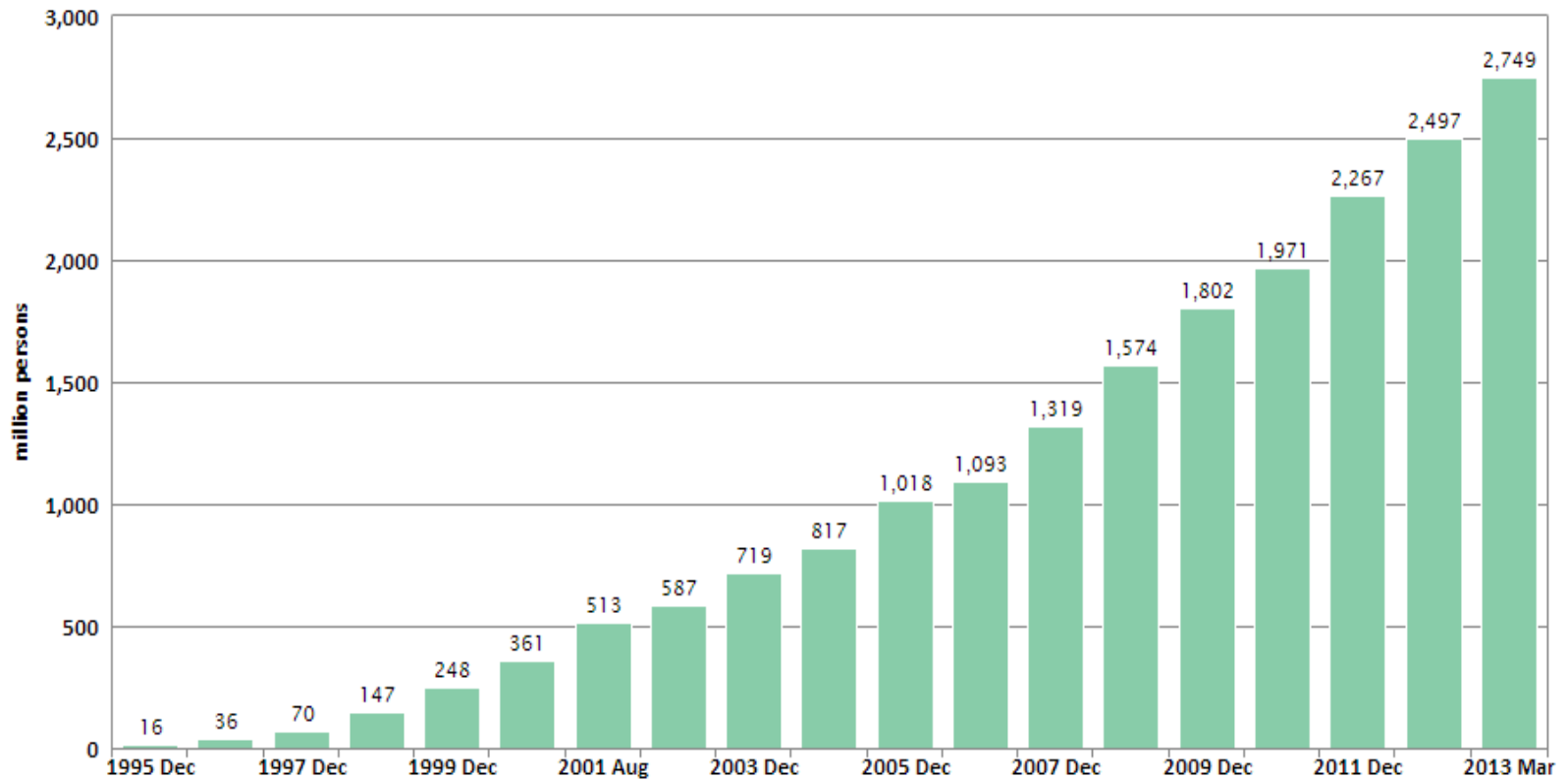


# Part 1: The idea of fighting cybercrime in the Fed. State of Hestia

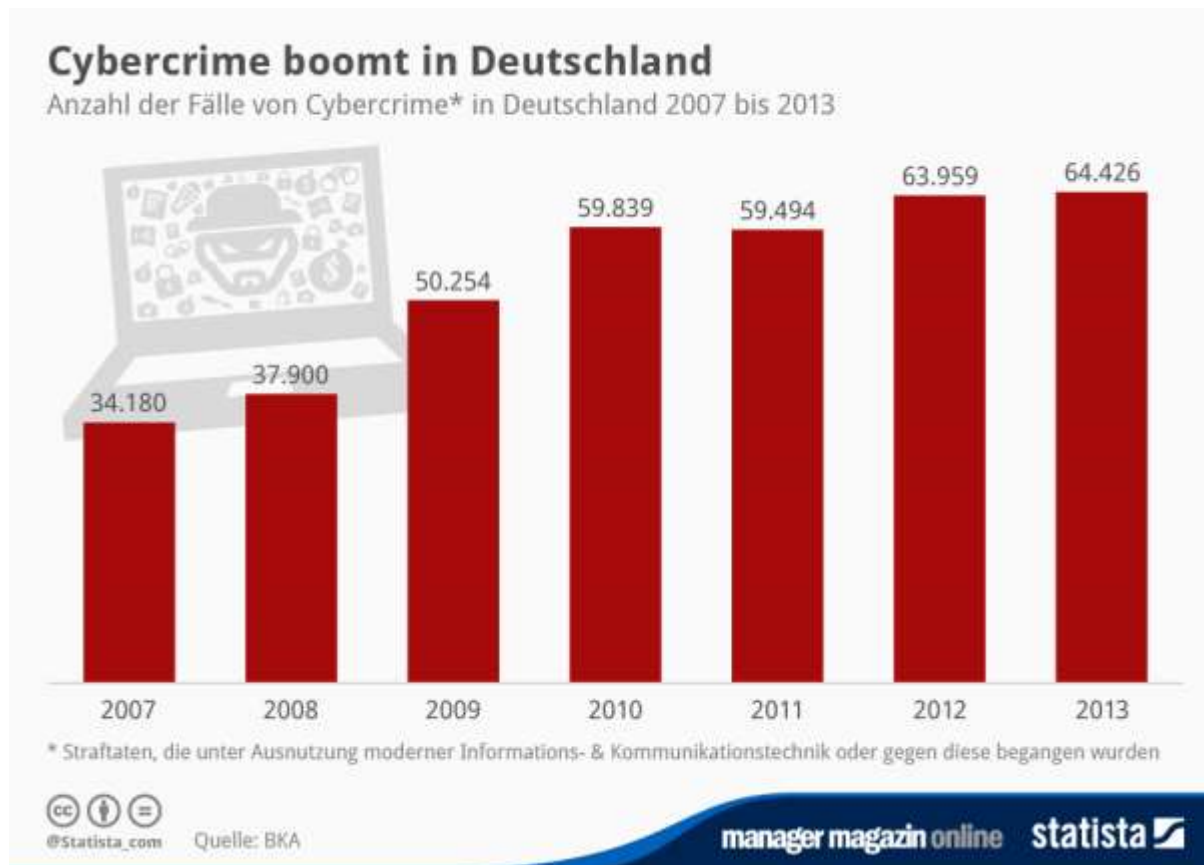


# The ages of the digital revolution

World Internet Usage Growth



# The actual relevance of cybercrime ist only insufficiently displayed in official statistics, real numbers remain largely unclear



# Estimations by the internet-industry



## The „Hessian“ concept on combatting cybercrime- Establishing specialized units

- Specialized units (prosecutors) on fighting cybercrime have been established inside of the District Attorney's offices (first one at the DA's office in Frankfurt 1999, followed by Marburg in 2001 and Giessen in 2002).
- Jan. 2010: Foundation of the Cybercrime-Center at the level of the Attorney General's office as a centralized and supervising unit.

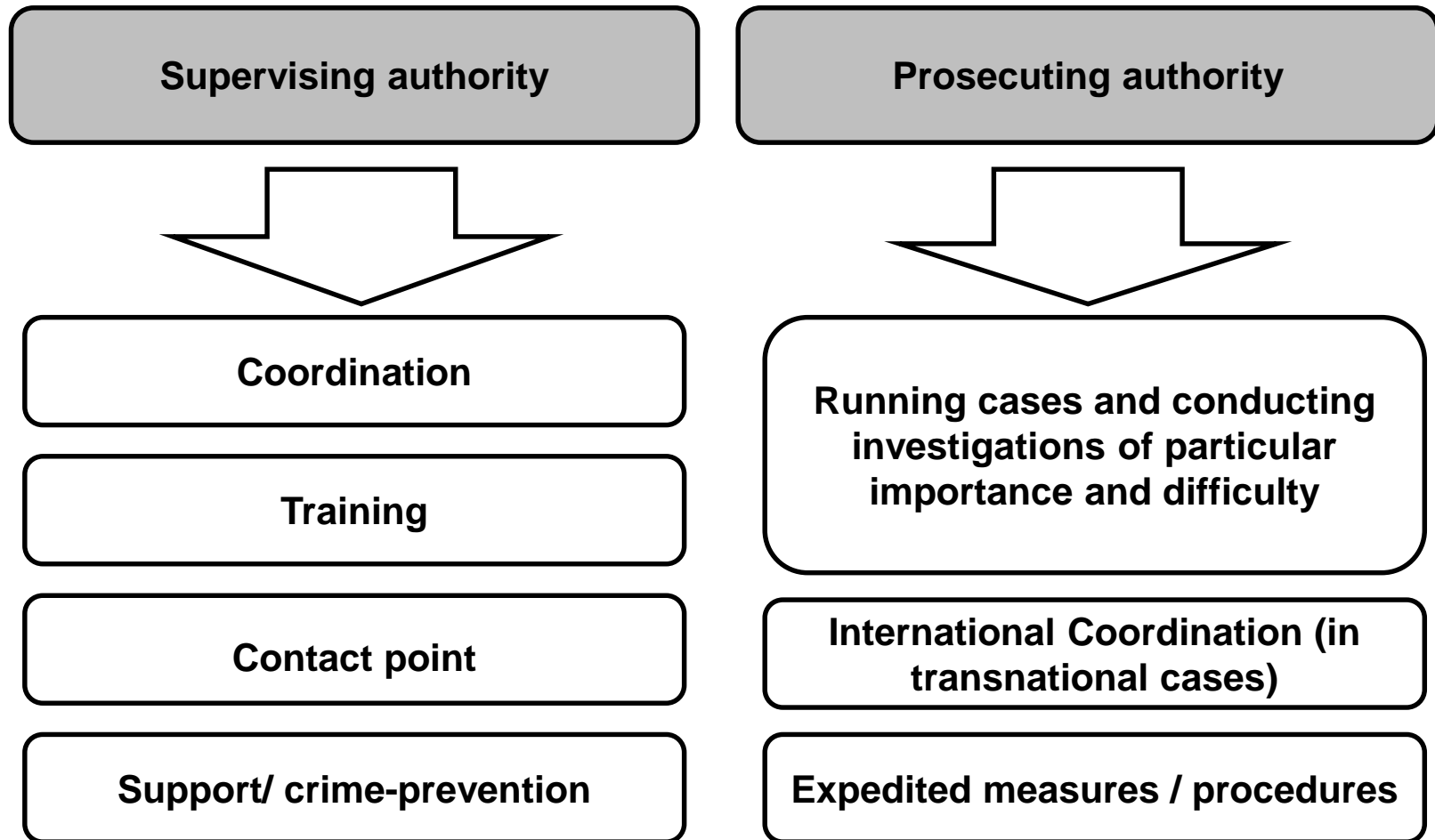
## Why establishing the Cybercrime-Center -

### Basic considerations :

- Cybercrime will be one of the most important and most demanding types of crimes in the nearer future. Globalization enhances this development.
- Since Cybercrime is subject to fast development, progress and adjustment, a specialized central unit can only match its expectations regarding coordination, training and support if it runs its own cases in order to enhance expertise and to stay up to date.



## Results of those considerations: 2 strings of tasks the cybercrime-center is charged with



## Organisation of the Cybercrime-center



- 5 highly experienced and specialized prosecutors, 1 senior prosecutor as head of office
- 24/7 stand-by-service
- modern technical equipment.

# Network



- Contact point for inquiries of the DA's offices
  - Access to the entire databases of the DA's offices
- Regular meetings for experience-sharing
- Inhouse-training-sessions for the DA's offices.

## Use of modern technologies



- Comprehensive electronic file management
- VPN-Access to the network from everywhere
- High-performance file-servers and encryption.

## Permanent acquisition and sharing of experiences and expertise



- Participation in national and international conferences and meetings,
- Permanent membership in various task-forces,
- Regular consultations with industry, banks and academics.

# National cooperation





# International cooperation



## Part 2: Cases being dealt with



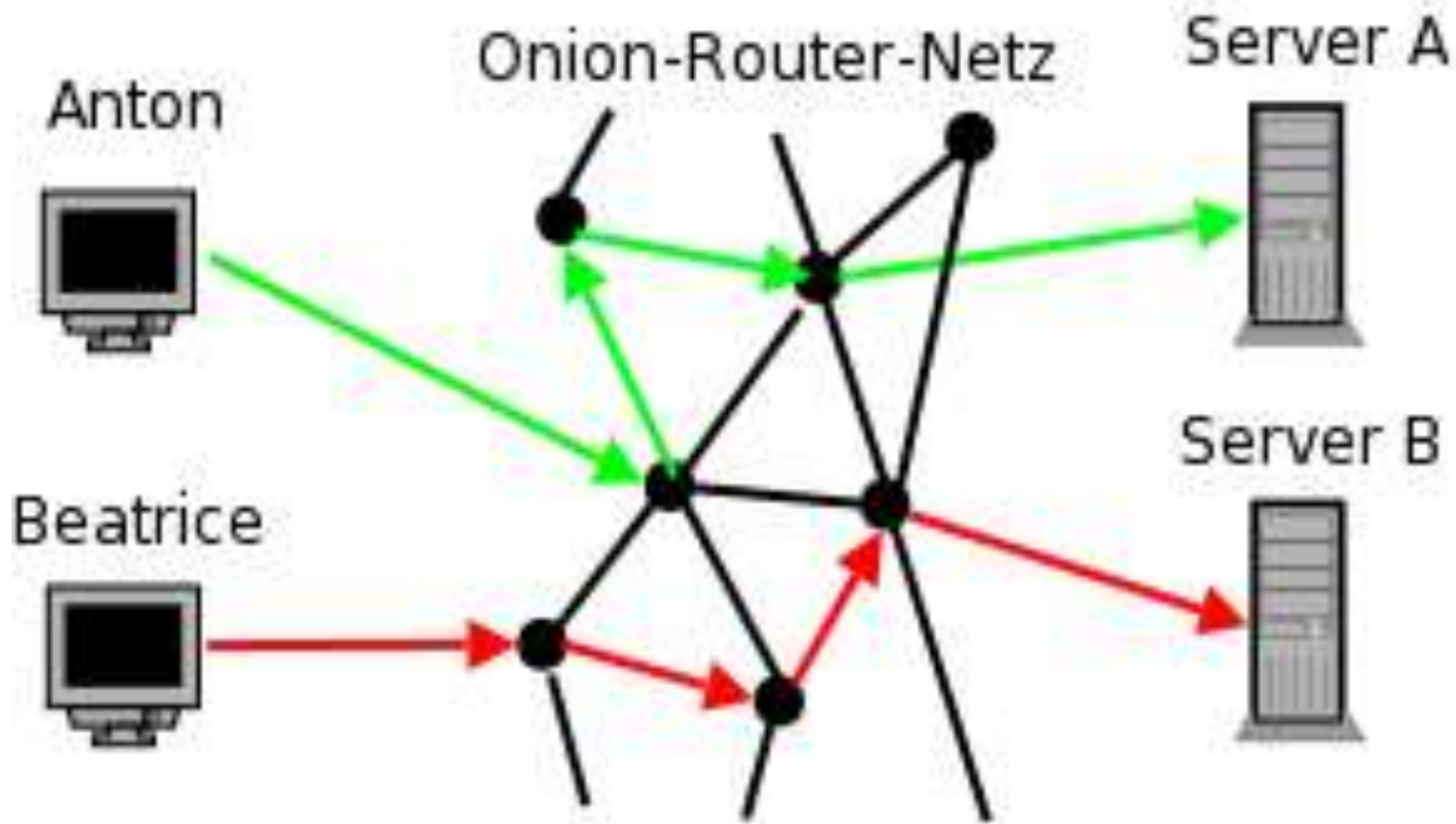


# Investigations on the Darknet

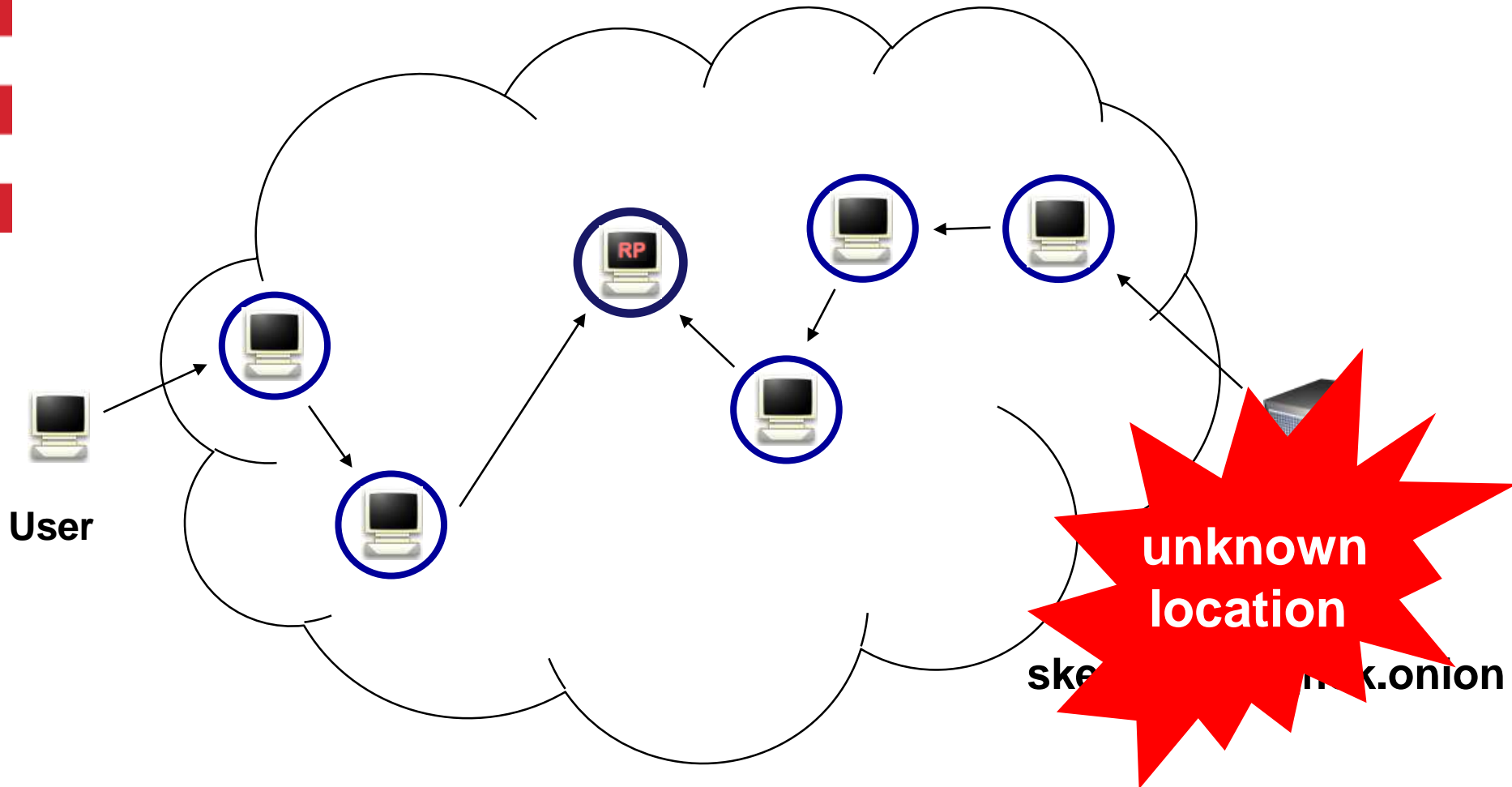




# The Onion Router (TOR)



# Darknet: TOR Hidden Services



# LE playgrounds – the big five





# Alp



[MS] Pistol Requests  
Item # 171167 - Pistols / Pistols - Paperchaser49 (337)

Views: 57927 / Bids: Fixed price  
Quantity left: Unlimited

Buy price  
USD 0.00  
(0.0000 BTC)



[MS] One Glock 26 with Extra Clip  
Item # 255875 - Pistols / Pistols - redface33 (68)

Views: 50643 / Bids: Fixed price  
Quantity left: Unlimited

Buy price  
USD 2,200.00  
(1.8496 BTC)



[MS] DefCad and FossCad 3D printable handguns  
Item # 196765 - Pistols / Pistols - User531 (72)

Views: 8194 / Bids: Fixed price  
Quantity left: Unlimited

Buy price  
USD 5.00  
(0.0042 BTC)



[MS] Glock 17 w Silencer  
Item # 44149 - Pistols / Pistols - Alexandra (95)

Views: 112432 / Bids: Fixed price  
Quantity left: Unlimited


Buy price  
USD 3,700.00  
(3.1106 BTC)

- Long-Range Guns 361
- Explosives 248
- Hand Weapons 430
- Other 517




[MS] Professional Tazer II 5000 K  
Volts  
Item # 116752 - Other / Other - Dutchdr

## Requirements



 **Tor-Browser-Paket**  
Version 6.0.4 | Rang 1 / 99 bei CHIP in der Kategorie: Anonymisierung

Windows Mac Linux

 **Download**  
Tor-Browser-Paket

**KOSTENLOS**

- ✓ Kostenlos
- ✓ Sicherer CHIP-Installer 



# Tor-Browser

Über Tor

Tor-Browser | Suche oder Adresse eingeben

Suchen

Das grüne Onion-Menü hat jetzt einen Sicherheitsschieberegler, mit dem Sie Ihre Sicherheitsstufe anpassen können. Probieren Sie es aus!

Öffne Sicherheits-Einstellungen

Tor-Browser 6.0



## Willkommen im Tor Browser

Sie können jetzt anonym im Internet surfen.

[Tor-Netzwerkeinstellungen testen](#)

Sicheres Suchen mit [Disconnect.me](#)

### Was nun?

Tor ist NICHT alles was benötigt wird, um anonym zu surfen! Sie müssen eventuell einige Gewohnheiten ändern, um sicherzustellen, dass Ihre Identität geschützt bleibt.

[Tipps, um anonym zu bleiben »](#)

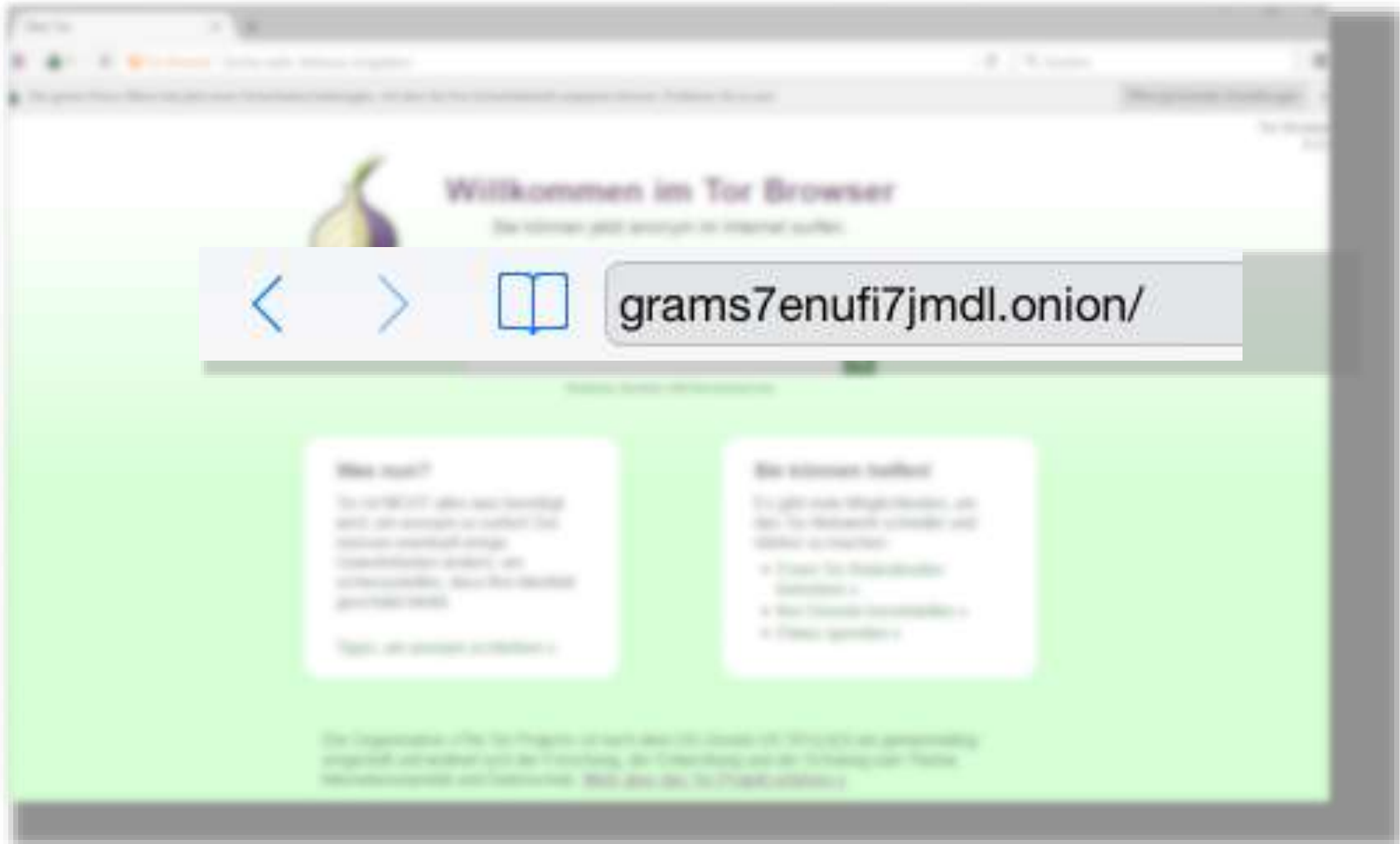
### Sie können helfen!

Es gibt viele Möglichkeiten, um das Tor-Netzwerk schneller und stärker zu machen:

- [Einen Tor-Relaisknoten betreiben »](#)
- [Ihre Dienste bereitstellen »](#)
- [Etwas spenden »](#)

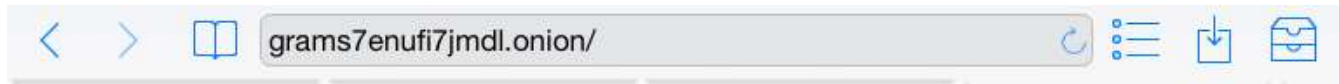
Die Organisation »The Tor Project« ist nach dem US-Gesetz US 501(c)(3) als gemeinnützig eingestuft und widmet sich der Forschung, der Entwicklung und der Schulung zum Thema Internetanonymität und Datenschutz. [Mehr über das Tor-Projekt erfahren »](#)

# Tor-Browser





# Grams...



Grams

Helix Helix<sup>light</sup> InfoDesk Login

## Search the darknet

Grams Search

I'm Feeling Lucky



InfoDesk

Search for a vendor or product



Helix<sup>light</sup>  
by Grams

No account, no entry fee, no PGP key verification



Flow  
by Grams

Flow allows you to easily get to hidden sites, e.g. type [gramsflow.com/agora](https://gramsflow.com/agora)

# Grams...

Grams   [Helix](#) [Login](#)

About 3828 results for 'Heroin' (0.5925 seconds)

[Advanced Search](#)



### 2 5g 3 Heroin brown Heroin

[pwoah7foa6au2pul.onion/listing.php?id=209290](#) **Alphabay**

**PRODUCT DESCRIPTION** 3 **Heroin** brown **Heroin** The 3 **Heroin** can be smoked on an aluminium foil snorted and injected if you dissolve it in water with citrus acid It gives you a warm and euphoric rush and you will feel narcotic if you consume more Every **heroin** user will appreciate this **heroin** and the price is more than fair for this quality level It is not high quality A but it is more strong than the stuff..

**Vendor** [Drogendealer](#) (0) **Price** ₿0.23118572 **Location** Germany



### 0 5g 3 Heroin brown Heroin

[pwoah7foa6au2pul.onion/listing.php?id=209288](#) **Alphabay**

**PRODUCT DESCRIPTION** 3 **Heroin** brown **Heroin** The 3 **Heroin** can be smoked on an aluminium foil snorted and injected if you dissolve it in water with citrus acid It gives you a warm and euphoric rush and you will feel narcotic if you consume more Every **heroin** user will appreciate this **heroin** and the price is more than fair for this quality level It is not high quality A but it is more strong than the stuff..

**Vendor** [Drogendealer](#) (0) **Price** ₿0.05107647 **Location** Germany

[Drogendealer](#) (0)



Set currency

**BTC**

USD

EUR

GBP

AUD



Market Chart



Market Status



Market Alerts

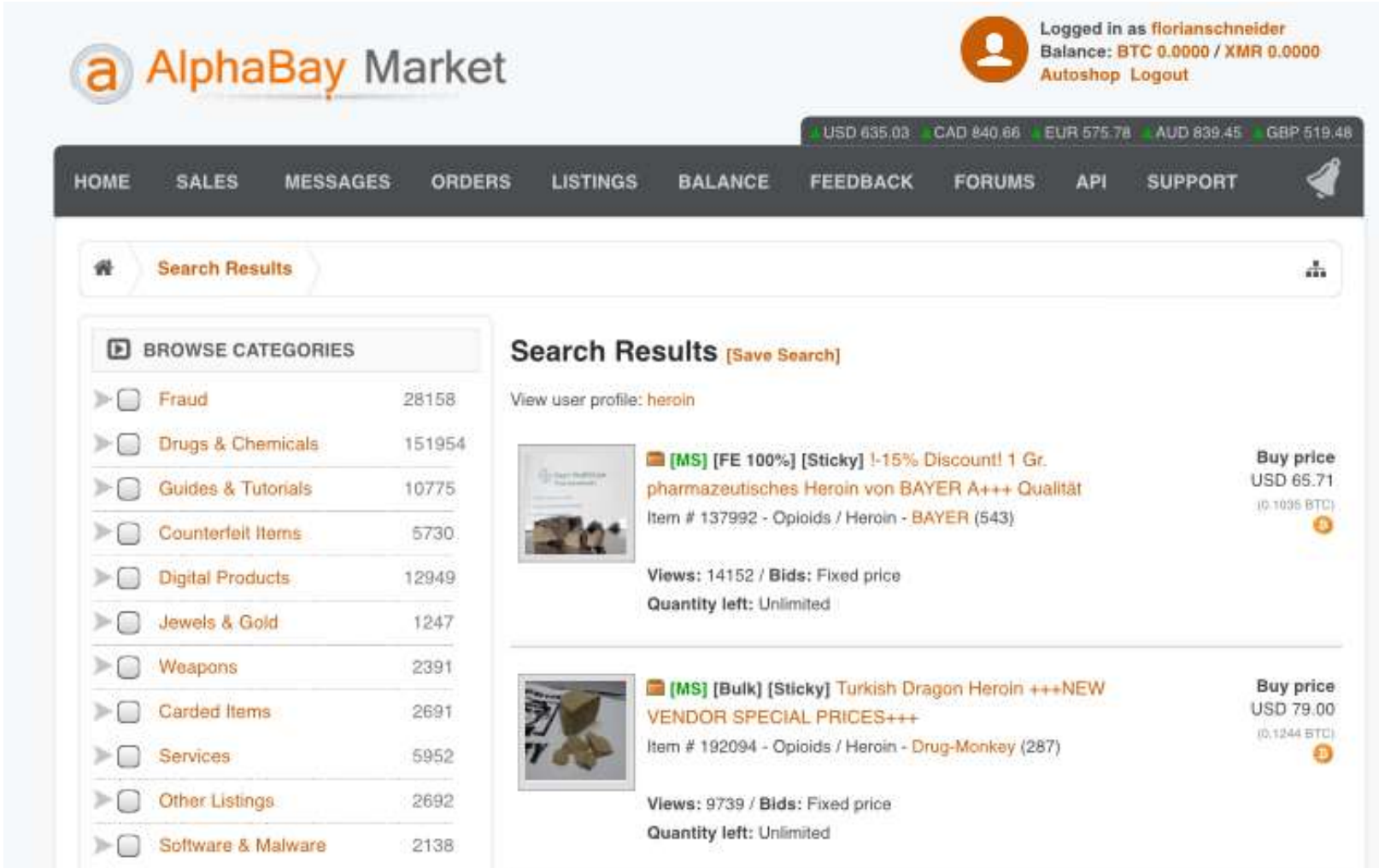
No Warnings

Also by Grams



Helix

# Drugs, drugs, drugs...



**AlphaBay Market**

Logged in as **fiorianschneider**  
 Balance: BTC 0.0000 / XMR 0.0000  
 Autoshop Logout

USD 635.03 CAD 840.66 EUR 575.78 AUD 839.45 GBP 519.48

HOME SALES MESSAGES ORDERS LISTINGS BALANCE FEEDBACK FORUMS API SUPPORT


**Search Results**

**BROWSE CATEGORIES**

Fraud	28158
Drugs & Chemicals	151954
Guides & Tutorials	10775
Counterfeit Items	5730
Digital Products	12949
Jewels & Gold	1247
Weapons	2391
Carded Items	2691
Services	5952
Other Listings	2692
Software & Malware	2138


**Search Results** [Save Search]

View user profile: [heroin](#)

 **[MS] [FE 100%] [Sticky] 1-15% Discount! 1 Gr. pharmazeutisches Heroin von BAYER A+++ Qualität**  
 Item # 137992 - Opioids / Heroin - BAYER (543)

**Buy price**  
 USD 65.71  
 (0.1035 BTC)

Views: 14152 / Bids: Fixed price  
 Quantity left: Unlimited

 **[MS] [Bulk] [Sticky] Turkish Dragon Heroin +++NEW VENDOR SPECIAL PRICES+++**  
 Item # 192094 - Opioids / Heroin - Drug-Monkey (287)

**Buy price**  
 USD 79.00  
 (0.1244 BTC)

Views: 9739 / Bids: Fixed price  
 Quantity left: Unlimited



...and even more drugs



**\*NO CUTS\* -1g- FIRST CLASS  
COCAINE FROM THE SOURCE  
\*FREE SHIPPING\* \*GER VENDOR\***

15% off for unspecified time 15% rabatt für unbestimmte zeit --  
perlweiss\_2016 hat jetzt auch haschisch und xtc im angebot  
natürlich nur feinste ware! perlweiss\_2016 has now first class  
hash and xtc! premium quality as always! VISIT OUR PROFILE ---  
2g -> choose quantity "2" at this listing! ---- 3.5g for 300\$ - 85\$/g  
<http://alphabaywyjrktqn.onion/listing.php?id=172171...>

Sold by **perlweiss\_2016** - 1001 sold since Jan 21, 2016 **Vendor**

**Level 7** **Trust Level 5**

	Features	Features
<b>Product class</b>	Physical p:	<b>Origin country</b> Germany
<b>Quantity left</b>	Unlimited	<b>Ships to</b> Europe,
<b>Ends in</b>	Never	Germany
	<b>Payment</b>	<b>FE Listing</b>

\*FREE SHIPPING\* \*DE\* - 1 days - USD +0.00 / order

Purchase price: USD 85.00

Qty:  **Buy Now**

0.1338 BTC / 12.4816 XMR

# Firearms

Grams


Helix Helix <sup>light</sup> InfoDesk Login

## Search the darknet

Grams Search

I'm Feeling Lucky

# Firearms




🔍


[Helix](#)   [Login](#)

About 428 results for 'Glock' (0.4373 seconds)


Advanced Search




**GLOCK 19 PEPPER PISTOL**  
pwoah7foa6au2pul.onion/listing.php?id=144155 **Alphabay**  
 Glock Pepper spray gun Range 5m 1 1 same like real **glock**  
**Vendor** [balkanpharma](#) (0)    **Price** ₿0.15332955    **Location** Worldwide



**NEW Glock 19 4th gen 3 MAGS**  
pwoah7foa6au2pul.onion/listing.php?id=100017 **Alphabay**  
 NEW **Glock** 19 4th generation Only 1 available Including 3 mags Original **glock** box Will be send with 2 shipments in parts Including easy manual on how to put it back together  
 Shipping to EU only FE required  
**Vendor** [FraudGod](#) (0)    **Price** ₿2.93470928    **Location** Worldwide



**Custom for Grim666Reaper**  
pwoah7foa6au2pul.onion/listing.php?id=41172 **Alphabay**  
 3 **Glock** 26 Slides and one **Glock** 26 barrell  
**Vendor** [Alexandrea](#) (60)    **Price** ₿4.46794251    **Location** Worldwide




Set currency

**BTC**    USD    EUR


GBP    AUD

---




Market Chart

---



Market Status


---



Market Alerts

No Warnings


Also by Grams



Helix


30

# ...all roads lead to AlphaBay



Logged in as **fiorianschneider**  
 Balance: BTC 0.0000 / XMR 0.0000  
 Autoshop Logout


USD 635.03
CAD 840.66
EUR 575.78
AUD 839.45
GBP 519.48

HOME
SALES
MESSAGES
ORDERS
LISTINGS
BALANCE
FEEDBACK
FORUMS
API
SUPPORT


**BROWSE CATEGORIES**

- Fraud 16386
- Drugs & Chemicals 78278
- Guides & Tutorials 6675
- Counterfeit Items 2889
- Digital Products 7259
- Jewels & Gold 741
- Weapons 1304
  - Ammunition 200
  - Pistols 449
    - Pistols 449
  - Long-Range Guns 127
  - Explosives 106
  - Hand Weapons 140
  - Other 282


## Search Results [\[Save Search\]](#)



**[MS]** (Clean) Colt 1911 -1972 Blue 70 Series .45 Auto  
 Item # 116132 - Pistols / Pistols - [howardstern](#) (7)

Views: 2450 / Bids: Fixed price  
 Quantity left: 1


**Buy price**  
 USD 350.00  
 (0.8413 BTC)



**[MS]** Pistols Australia + Ammo & Accessories  
 Item # 113910 - Pistols / Pistols - [pillmonsta](#) (6)

Views: 235 / Bids: Fixed price  
 Quantity left: Unlimited

**Buy price**  
 USD 3,663.07  
 (8.8055 BTC)




**[MS]** Weapons Marketplace: [guntrawb2upat3nm.onion](#)  
 Item # 121957 - Pistols / Pistols - [GunTrade\\_Official](#) (2)

Views: 0 / Bids: Fixed price  
 Quantity left: 4

**Buy price**  
 USD 1.00  
 (0.0024 BTC)

# Thus, the place to be for Organized Arms-traffickers



## Custom listing for Irerl5

MAADI AK47

Sold by [goods2you](#) - 2 sold since Aug 29, 2016 Vendor Level

1 Trust Level 3

	Features	Features
Product class	Physical p	Origin country
Quantity left	Unlimited	Ships to
Ends in	Never	Payment
		Escrow

Worldwide

Worldwide

Escrow

Default - 1 days - USD +100.00 / item

Purchase price: USD 4,000.00

Qty:  Buy Now

฿5774 BTC / 383.5091 XMR





# Trade in counterfeit

**20 EURO whmx counterfeit**   **20 dollar whmx counterfeit**   **20 EURO whmx counterfeit**   **20 dollar whmx counterfeit**

**whmx dollar counterfeit**

**HIGH QUALITY**

**8 Security features (same as original)**

**20 DOLLARS COUNTERFEIT**  
**PRICE: 0,5 BTC / BILL**  
MIN ORDER: 25 SHIPPING: 1,5BTC

Production: 9000 monthly our production rate is way to high to spend all the notes ourselves.

Information / Order: [whmx20@tormail.org](mailto:whmx20@tormail.org)   Acrimonious Escrow Accepted

**20 EURO Counterfeits**  
**PRICE: 0.6 BTC / Unit**  
Min order: 25   Shipping : 1BTC  
Shipping from France




Information / Order: [whmx20@tormail.org](mailto:whmx20@tormail.org)   Acrimonious Escrow Accepted

Use GPG in your email client to encrypt your emails.  
 GPG Fingerprint: B679 28EB 4810 D1C2 D266 85C7 8EA7 832F 4432 CB08  
[Download WHMX GPG Key \(4432CB08\)](#)

# Trade in forged official documents

## `German Passports`



<b>Price</b>	119.23066 BTC
	 \$ 1,279.50  £ 800.89  € 1,000.00
<b>Ship from</b>	Germany
<b>Ship to</b>	worldwide
<b>Stock</b>	100
<b>Created in</b>	2012-11-01 15:58 UTC
<b>Last update</b>	2012-11-03 11:19 UTC

*Your balance isn't enough to buy this item! Please deposit the needed funds before.*

### Description

German Passport - after you bought the passport you have to send me your information which should come on the passport incl. Photo.

identical passport - like an original!

Passport is produced within 5-8 days and will be sent with DHL (+trackingnumber), shipping for free.

# Trade in official documents



Onion-ID

[Main](#) [Pictures](#) [Prices](#) [FAQ](#) [Contact](#)

Want to ...

- ... *drive or rent a car anonymously?*
- ... *open bank accounts anonymously?*
- ... *open a P.O.Box anonymously?*
- ... *rent an apartment/house anonymously?*
- ... *send/recieve Westernunion payments anonymously?*

**Then get your 2nd identity from us!**

NEWS:

Here are some more, better tagged pictures to show that we are the original and that other guy on hidden wiki is just copying us.



# Crime-as-a-Service

## Crime Areas

### CRIME AS A SERVICE

- Infrastructure-as-a-Service
- Data-as-a-Service
- Pay-per-install Services
- Hacking-as-a-Service
- Translation Services
- Money-Laundering-as-a-Service


### MALWARE

- Trojans
- Criminal Botnets



# DDoS-attacks

Posted 23 August 2015 - 08:54 PM



**2nd LVL**  
504 posts  
Member since: 21-August 15

## CRIME NETWORK UNLEASHED SCENE

### Webserver

- Keine Bekanntheit, sowie kein Schutz: 10€ BTC / 1std
- Keine Bekanntheit aber Schutz: 15€ BTC / 30min
- \*Bekanntheit sowie Schutz: 25€ BTC / 30min
- \*Massenbekanntheit sowie Schutz: 35€ BTC / 30min

### Teamspeak3

- Keine Bekanntheit, sowie kein Schutz: 11€ BTC / 1std
- Keine Bekanntheit aber Schutz: 16€ BTC / 30min
- \*Bekanntheit sowie Schutz: 26€ BTC / 30min
- \*Massenbekanntheit sowie Schutz: 36€ BTC / 30min

### Gameserver/VPS

- Keine Bekanntheit, sowie kein Schutz: 12€ BTC / 1std
- Keine Bekanntheit aber Schutz: 17€ BTC / 30min
- \*Bekanntheit sowie Schutz: 27€ BTC / 30min
- \*Massenbekanntheit sowie Schutz: 37€ BTC / 30min

### Privatpersonen

- Normale externe IP: 5€ BTC/1std
- VPN: 10€ BTC/1std
- VPN (DDoS Protected): 15€ BTC/1std



# DDoS-attacks

FAQ:

**§1: Was für Equipment benutzt du für die ganzen Angriffe?**

Hauptsächlich Bots, bei kleineren Seiten/Gameserver benutze ich meine Server.

**§1.1: Was soll ich machen wenn sich die IP-Adresse bei der Privat Person geändert hat?**

Wenn ihr beispielsweise einen 2 Stunden DDoS Service für eine Privatperson beantragt habt, dieser jedoch nach 1 Stunde eine neue IP hat (wg. dynamisch) müsst ihr mir die neue IP schicken.

**§2: Sind die Preise oben festgelegt?**

Ja, Jedoch gibt es eine Ausnahme bei den Preisen wenn einer den Service auf dauer in Anspruch nimmt oder mehrere IP's gleichzeitig gehittet haben will.

**§2.1: Kann ein Webserver suspendiert werden wenn er die ganze zeit Angegriffen wird?**

Ja, Er kann in der tat suspendiert werden wenn ein dauerangriff durchgeführt wird.

**§3: Wie lange darf ein Angriff pro tag ausgeführt werden?**

Ich habe es so festgelegt, dass ein User pro Tag maximal 12 Stunden beantragen kann, Es hat nämlich den Grund, dass ich diesen Service nicht nur für eine Person anbiete, sondern es jeden recht machen will.  
Ausnahme: Siehe FAQ §2

**§3.1: Wann bist du immer online?**

Montag: 13:00 - 16:00 | 23:30 - 3:00  
Dienstag bis Freitag: 16:00 - 3:00  
Samstag bis Sonntag: 15:30 - 5:00

**§4: Wie kann man dich kontaktieren?**

CNW eine Private Nachricht schreiben.

Jabber: [REDACTED]

ICQ: [REDACTED]

Skype: [REDACTED]

**§4.1: Was hat die Whitelist zu bedeuten?**

Auf der Whitelist sind die Leute, die dafür bezahlen um nicht Angegriffen zu werden.  
Der Bezahlvorgang ist nur einmalig.

# Hitman services



**Quick Kill**

\$20,000, 50% before job and 50% after. This is necessary.

We target regular citizens. We do not target political figures or anyone under the age of 18.

We accept Bitcoin and Liberty Reserve.

We are here to do business.

We send you proof when the job is done.

Contact [██████████@tormail.net](mailto:██████████@tormail.net) or use the contact form. Remember to include your e-mail address when using the contact form.

Remove the problem from your life.

# Trade in stolen identities and data

08-05-2011 05:56 AM

**Selling 11Million UK DOB database \$25k**

Subject. CSV file 618mb, 11098605 lines.

Sample:

- "Rebecca [REDACTED]", "1979-03-18", "Bavaria", "B1929"
- "Alan [REDACTED]", "1961-12-14", "Derby", "DE23 3XB"
- "Robert [REDACTED]", "1970-05-20", "Bexley", "DA5 2AW"
- "Clare [REDACTED]", "", "Bexley", "DA5 2AW"
- "Pamela [REDACTED]", "1964-06-07", "Littlehampton", "BN16 3AU"
- "Jeremy [REDACTED]", "1979-03-24", "London", "NW11 8SR"
- "Mirjam [REDACTED]", "", "London", "NW11 8SR"
- "David [REDACTED]", "1988-11-09", "Swinton", "M27 6AS"
- "Michael [REDACTED]", "1947-05-13", "Worsley", "M28 3NJ"
- "Michael [REDACTED]", "1966-07-19", "Thame", "OX9 3PN"

My price is \$25k.

You can do simple search thru this base quickly, Also you can start your own dob search service - i can do a website for you for just \$1000 (with liberty reserve, webmoney payment system).

Only serious clients.  
Will sell only in 1 (ONE) hands.  
Contact via jabber: [REDACTED]

★ ⚠

Reply Reply With Quote



# Mechanisms of darknet-markets: The rating-systems

Profile



★ 

**Account Type**  
Level 2 Seller

**Seller Status**  
Active

**Member since**  
2013-01-11

**Last seen**  
2013-02-15

**Feedback**  
32

**Favorited**  
19 times

[view listings](#)

About the user

*This user hasn't write nothing about himself yet!*

Feedback

<< 1 2 3 4 >>

From	Rate	User As	Message	Title
<a href="#">theduke71</a>	●	seller	Goods as advertised and a nice guy	( ' 5x Party Flock (purple)...
<a href="#">cizia</a>	●	seller	Ok all good. 5/5 thanks bro...	( ' 1x Party Flock (purpl...
<a href="#">experience2080</a>	●	seller	Excellent, fast shipping. Thanks.	( ' 1,0gr Very Pure Cocaine...
<a href="#">justjohn</a>	●	seller	good seller, good delivery	( 'Very Pure Cocaine 80% ...
<a href="#">pindulinka</a>	●	seller	Arrived and I am happy, satisfied, thanks A+	( 'Very Pure Cocaine 80% ...
<a href="#">13White Widow37</a>	●	seller	He Sent at Friday and I received it Wednesday. Really good Product! Recommended for MDMA and Pill Lovers :)	( ' 1 x Party Flock (purp...
<a href="#">freedom88</a>	●	seller	thnx :)	( ' 10x 20 euro notes COUN...
<a href="#">cardplastk</a>	●	seller	good bro , honest seller!	( ' SpyEye Botnet v.1.3.48...
<a href="#">maarten0</a>	●	seller	nice stuff :) - thank you:)	( ' 0,5gr Very Pure Cocaine...
<a href="#">gaumeland</a>	●	seller	Very nice sample of real cocaine...	( 'Very Pure Cocaine 80% ...



# Mechanisms : The delivery of purchased goods



el-basar.biz
Support: 419-969-356

**PACKSTATION**  
instant and safe order.

user Login

Username

\*\*\*\*\*

login

**Drugs wieder verfuegbar**

Guten Tag liebe Kunden,

wir haben uns entschieden Drugs wieder zu Top Qualität anzubieten.  
Das Pepp ist voll konkurrenz fähig und wird mit garantie die beste Qualität, die im Internet angeboten wird sein.

In ferner Zukunft werden wir zusätzlich auchnoch XTC Pillen anbieten, perfekt für den eigenen Konsum oder zum weiterverkaufen an die Ticker in eurer Umgebung :).

Mit freundlichen Grüßen El-basar.biz

2011-04-04 21:51:39

# Mechanisms of the darknet-markets: The payment



# Mechanisms of the darknet-markets: The payment





# CryptoLocker

CryptoLocker
⌵

## Your personal files are encrypted!



Private key will be destroyed on  
**9/8/2013**  
**5:52 PM**

Time left:  
**56 : 16 : 12**

Your important files **encryption** produced on this computer: photos, videos, documents, etc. [Here](#) is a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a **unique** public key **1155-2048** generated for this computer. To decrypt files you need to obtain the **private key**.

The **single copy** of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will **destroy** the key after a time specified in this window. After that, **nobody and never will be able** to restore files...

**To obtain** the private key for this computer, which will automatically decrypt files, you need to pay **100 USD / 100 EUR /** similar amount in another currency.

Click **<Next>** to select the method of payment and the currency.

**Any attempt to remove or damage this software will lead to the immediate destruction of the private key by server.**

# Cybercrime and „Underground Economy“

# OP Onymous



# OP Onymous



U.S. Immigration and  
Customs Enforcement



## THIS HIDDEN SITE HAS BEEN SEIZED

as part of a joint law enforcement operation by  
the Federal Bureau of Investigation, ICE Homeland Security Investigations,  
and European law enforcement agencies acting through Europol and Eurojust

In accordance with the law of European Union member states  
and a protective order obtained by the United States Attorney's Office for the Southern District of New York  
in coordination with the U.S. Department of Justice's Computer Crime & Intellectual Property Section  
issued pursuant to 18 U.S.C. § 983(j) by the  
United States District Court for the Southern District of New York



## OP Onymous: Action Day 6. November 2014

- Cooperation of 16 EU-countries and several U.S LE-authorities, coordinated through EUROPOL and EUROJUST
- Seizure of 600+ onion-domains for hidden services,
- Splash-pages uploaded onto 414 onion-domains,
- 17 admins and vendors being arrested,
- 13 house searches
- Confiscation of \$ 1 Mio. in bitcoin etc.





## Investigations against German vendors on darknet-marketplaces


- Transfer of relevant data on different marketplaces from the U.S. to European LE through EUROPOL EC3
- Analysis of the data provided done by the domestic LE-authorities.
- Several cases initiated against German vendors and powersellers.
- After conducting the initial investigations, single cases being submitted to the relevant local prosecution offices.

## Cybercrime and „Underground Economy“

# Operation Blackshades



# Malware Blackshades- Trojan for everybody



## Cybersecurity Threat:

# Blackshades RAT








**Quick facts:**

- Blackshades RAT is a new and powerful crimeware remote access tool that infects windows devices
- An FBI-led crackdown has arrested more than 90 individuals worldwide
- The threat remains to individuals and enterprises
- Blackshades RAT lets criminals spy on you and control your device

**Uses:**

- launch attacks
- stealth surveillance
- extortion
- spread infection
- identity theft
- blackmail
- keylogging
- hard to detect
- mouse tracking
- webcam spying
- screen capture
- lockouts

**The 7 signs of infection: \***

	<b>Mouse</b> cursor moves erratically		<b>Webcam</b> light unexpectedly turns on
	<b>Monitor</b> turns off while in use		<b>Passwords</b> online accounts have been compromised
	<b>Money</b> unauthorized logins to bank accounts		<b>Chat</b> chat windows appear unexpectedly
	<b>Ransom</b> ransom demand is made to unlock files	<b>Learn more at:</b> <a href="http://www.stateoftheinternet.com/blackshades">www.stateoftheinternet.com/blackshades</a>	

\* "Blackshades MalwareTakedown", FBI, 19 May 2014.



# Blackshades

Process Name	Path	Private	Working Set	Private Bytes	
svchost.exe	C:\Program Files\Microsoft\Windows\Software\svchost.exe	1488	6	Normal	5,931 KB
svchost.exe	C:\Windows\System32\svchost.exe	1532	27	Normal	14,438 KB
MsMpEng.exe	C:\Program Files\Microsoft Security Center\MSMpEng.exe	1644	10	Normal	4,471 KB
MsMpEng.exe	C:\Program Files\Microsoft Security Center\MSMpEng.exe	1776	43	High	36,238 KB
svchost.exe	C:\Program Files\Microsoft\Windows\Software\svchost.exe	1920	16	Normal	5,734 KB
svchost.exe	C:\Program Files\Microsoft\Windows\Software\svchost.exe	2036	19	Normal	4,951 KB
svchost.exe	C:\Program Files\Microsoft\Windows\Software\svchost.exe	1672	9	Normal	6,221 KB
svchost.exe	C:\Program Files\Microsoft\Windows\Software\svchost.exe	2794	21	Normal	5,714 KB
svchost.exe	C:\Windows\System32\svchost.exe	2460	0	Normal	4,021 KB
svchost.exe	C:\Windows\System32\svchost.exe	2460	0	Normal	5,671 KB
svchost.exe	C:\Windows\System32\svchost.exe	3520	3	High	25,448 KB
svchost.exe	C:\Windows\System32\svchost.exe	2388	2	Normal	2,118 KB
svchost.exe	C:\Program Files\Microsoft\Windows\Software\svchost.exe	3060	6	Normal	1,361 KB
svchost.exe	C:\Windows\System32\svchost.exe	2294	23	Normal	30,238 KB
svchost.exe	C:\Program Files\Microsoft\Windows\Software\svchost.exe	3528	4	Normal	6,431 KB
svchost.exe	C:\Program Files\Microsoft\Windows\Software\svchost.exe	3236	11	Normal	10,748 KB
svchost.exe	C:\Windows\System32\svchost.exe	3236	3	Normal	6,301 KB
svchost.exe	C:\Windows\System32\svchost.exe	3520	3	Normal	6,471 KB
svchost.exe	C:\Program Files\Microsoft\Windows\Software\svchost.exe	3328	2	Normal	6,411 KB
svchost.exe	C:\Windows\System32\svchost.exe	3364	4	Normal	6,341 KB
svchost.exe	C:\Program Files\Microsoft\Windows\Software\svchost.exe	2408	0	Normal	1,371 KB
svchost.exe	C:\Program Files\Microsoft\Windows\Software\svchost.exe	3448	15	Normal	30,848 KB
svchost.exe	C:\Windows\System32\svchost.exe	2436	2	Normal	6,391 KB
svchost.exe	C:\Program Files\Microsoft\Windows\Software\svchost.exe	3732	46	Normal	79,948 KB
svchost.exe	C:\Program Files\Microsoft\Windows\Software\svchost.exe	3524	4	Normal	5,251 KB
svchost.exe	C:\Windows\System32\svchost.exe	2952	2	Normal	4,921 KB
svchost.exe	C:\Program Files\Microsoft\Windows\Software\svchost.exe	2060	1	Normal	4,421 KB
svchost.exe	C:\Program Files\Microsoft\Windows\Software\svchost.exe	3320	10	Normal	18,148 KB
svchost.exe	C:\Program Files\Microsoft\Windows\Software\svchost.exe	3716	11	Normal	14,438 KB

## Webcam

The Webcam feature is really easy to use, simply right click on the bot you want and select Webcam Manager. You can vary the quality of the webcam depending on how fast your connection is, lower quality = less data used = less jerky but also less clear. Select Save if you want to save the feed, it is however saved in pictures rather than as a video.

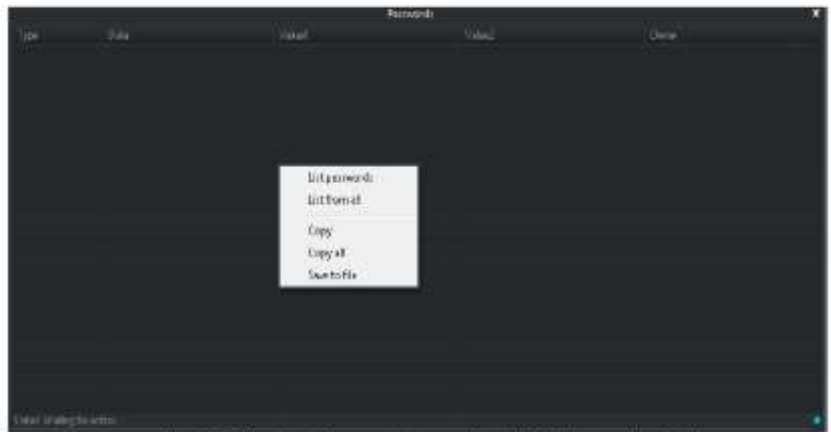
Quality at 100



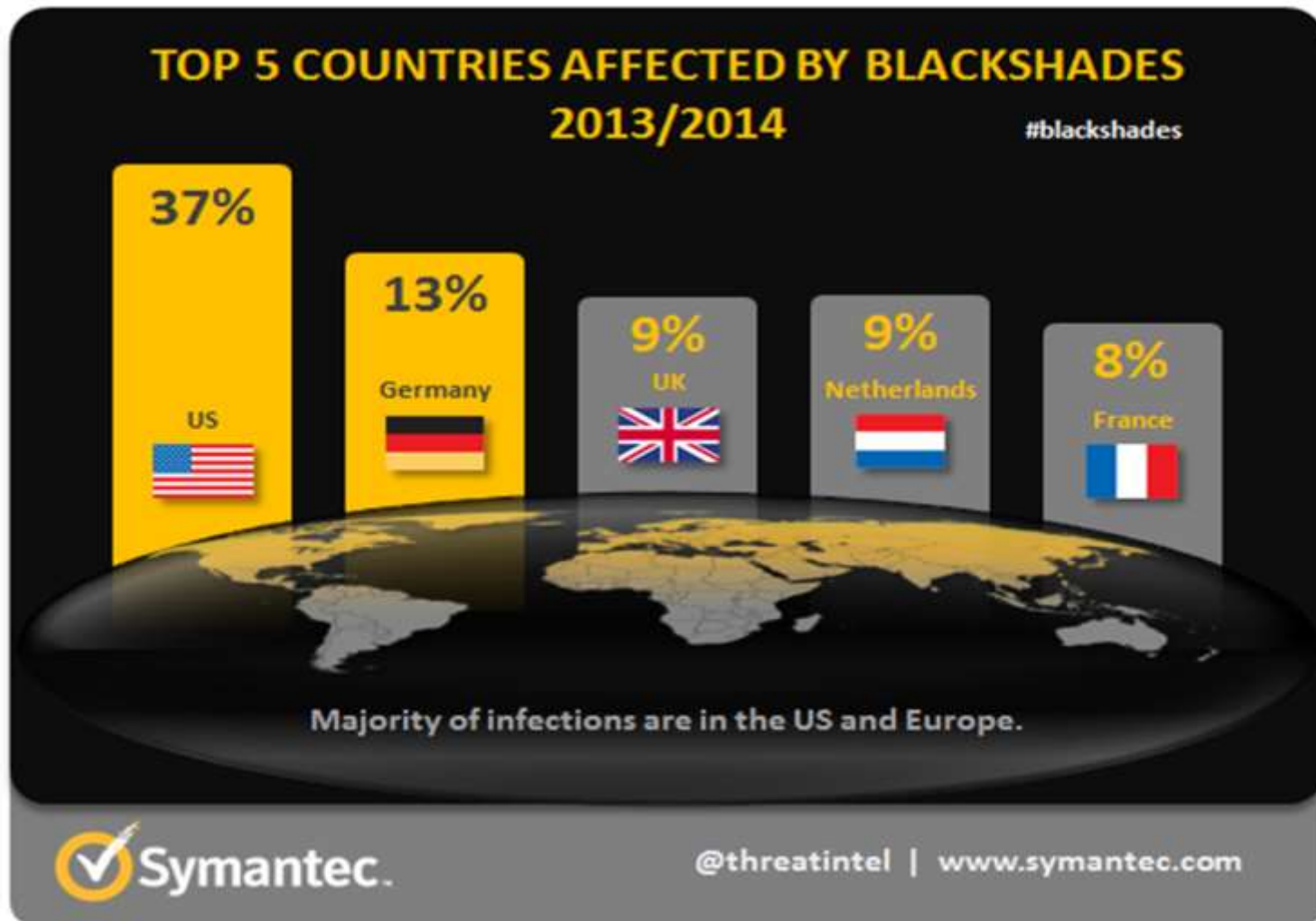
Quality at 50



## Passwords



# BS – distribution



## Operation „Dirty R.A.T.“

- Internationally coordinated approach
- Worldwide „Action Day“ on 13.05.2014
- 19 countries involved
- Operations center in The Hague
- 157 search-and-seizure warrants secured and executed in Germany.





# THIS DOMAIN HAS BEEN SEIZED

by the Federal Bureau of Investigation in accordance with a seizure warrant obtained by the United States Attorney's Office for the Southern District of New York and issued pursuant to 18 U.S.C. § 981 by the United States District Court for the Southern District of New York.



## Cybercrime and „Underground Economy“

# Bitcoin-Mining



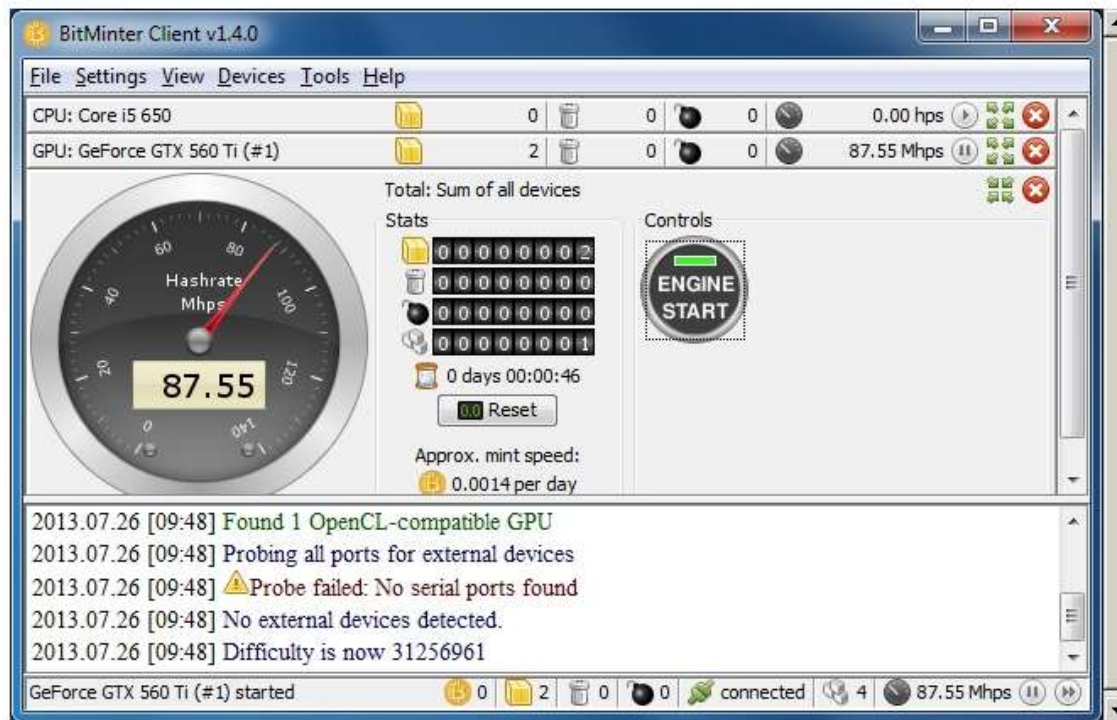


## „Bitcoin-Mining“

- Bitcoin is a digital currency, independent from banks and official regulation
- Bitcoins are assigned to digital wallets through cryptographic keys.
- Bitcoins are regularly used for purchasing goods on online-platforms
- Bitcoin allows for international transactions
- Bitcoins can be exchanged into „real“ money.

# „Bitcoin-Mining“

- Bitcoins are being produced by processing and resolving highly complex mathematical equations („mining“)
- Installation of a special mining-client required („bitcoin-client“)

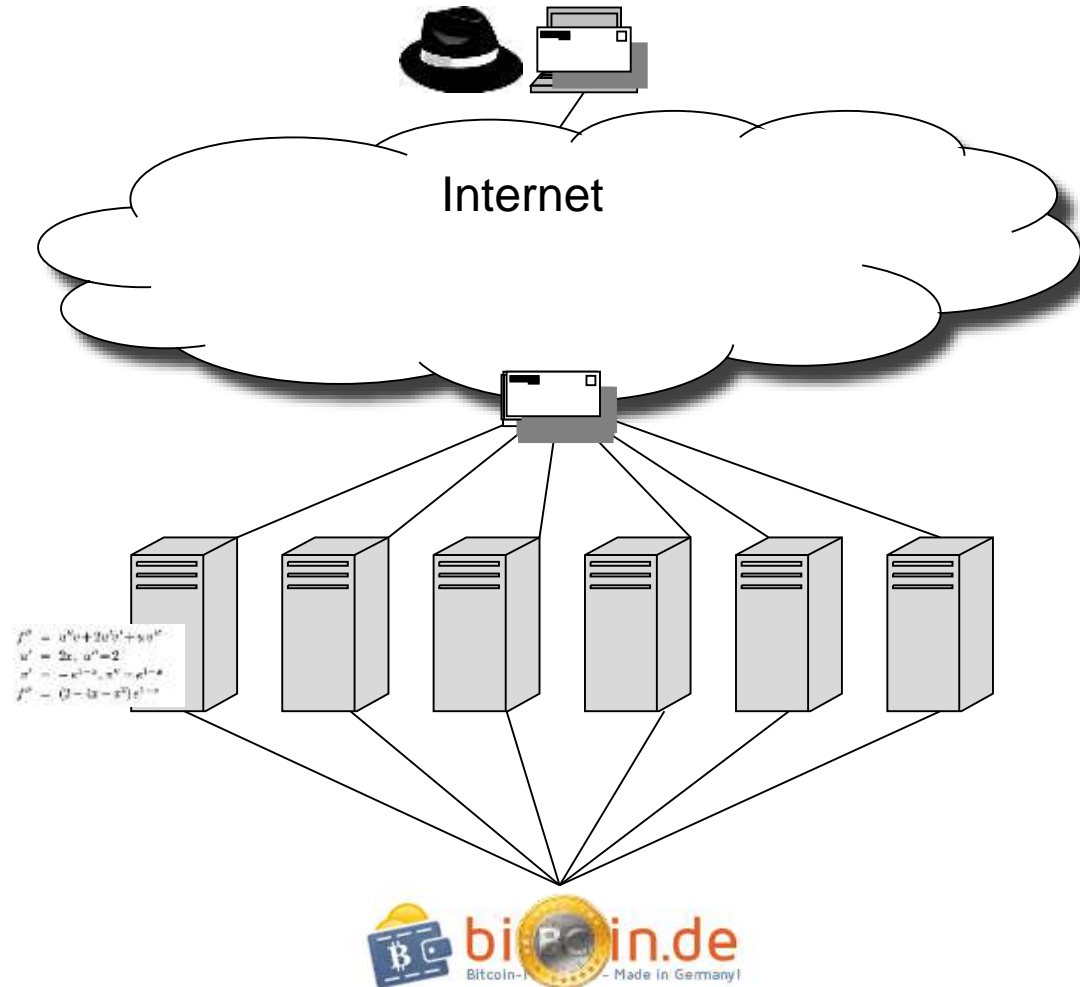


BitMinter ist eines der Programme mit denen sich das digitale Gold der Bitcoins schürfen lässt.

## „Bitcoin-Mining“

- **But:** Mining on a standard computer takes years
- Costs for electric power used by the computer exceeds the profit to be gained by mining
- Thus: special high-performance computers are required for efficiently mining bitcoins.
- Solution for criminals: **Mining through botnets**

# „Bitcoin-Mining“



# „Bitcoin-Mining“

## Results of the investigations:

- Perpetrator („Manager“) disclosed his ICQ-number to Undercover Agents.
- Subscriber data request successful, since „Manager“ used same IP over several weeks
- Wiretapping disclosed additional complices

## „Bitcoin-Mining“

### results:

- 2012: Distribution of nearly 50 Mio. infected datasets
- Malware is being adjusted daily
- Ca. 1000 new infections each day
- Computing power of relevant botnet amounted to 2 petaflop
- Produced bitcoins being exchanged into „real“ money
- Net profit: 15.000 Euros per month

# „Bitcoin-Mining“

## Problems:

- Mere production of bitcoins is not punishable!
- Infection of computers constitutes a crime under German criminal code
- But this is only considered a minor crime
- Thus: German procedural code does not provide for wiretapping in those cases!

# Operation Rico





## Operation rico

# Das Protokoll der Münchner Amok-Nacht

Ein 18-jähriger Schütze tötet am 22. Juli 2016 neun Menschen und begeht anschließend Selbstmord



## Operation Rico

# Das Protokoll der Münchner Amok-Nacht

Ein 18-jähriger Schütze tötet am 22. Juli 2016 neun Menschen und begeht anschließend Selbstmord



## Operation Rico

# Das Protokoll der Münchner Amok-Nacht

Ein 18-jähriger Schütze tötet am 22. Juli 2016 neun Menschen und begeht anschließend Selbstmord



Pistole vom Typ Glock 17



## Operation Rico

# Das Protokoll der Münchner Amok-Nacht

Ein 18-jähriger Schütze tötet am 22. Juli 2016 neun Menschen und begeht anschließend Selbstmord



# Die Glock aus dem Darknet

**Kriminalität** Wie konnte sich ein 18-jähriger Junge eine scharfe Pistole für ein geplantes Attentat im Internet besorgen? Der Verfolgungsdruck auf Waffenhändler nimmt zu.



Pistole vom Typ Glock 17

## Course of investigations

Account „E.“ previously taken over by LE

**04.07.2016** – first contact from user „S.“ on DDW

**22.07.2016** – first contact from user „T.“ on DDW

**27.07.2016** – Take-over of account „S.“

**02.08.2016** – Take-over of account „T.“

**05.08.2016** – first contact to „rico“ through „S.“

**05.08.2016** – link from „rico“ to the spree shooter  
established

**16.08.2016** – apprehension of „rico“



# Deutschland

Informationskontrolle, nein danke!



[Übersicht](#)
[Tabber/Cryptocat](#)
[Webchat \(15\)](#)
[Bitcoin \(522 EUR\)](#)
[MultiSig Escrow](#)
[Spenden](#)
[Suche](#)
[Profil](#)
[Abmelden](#)

Angemeldet als **elsien**.
 
[Neue Beiträge](#)
[Aktive Themen](#)
[Unbeantwortete Themen](#)
[Abonnements](#)
[Nachrichten](#)

Deutschland im Deep Web > Profil von **rico**

Willkommen im Profil von **rico**

<b>rico</b>	Registrierungsdatum: <b>07.11.2013</b>
<b>Kennt sich aus</b>	Letzter Beitrag: <b>07.07.2016 18:34:00</b> Beiträge: <b>146</b> Danke erhalten: <b>20</b>
<b>Kontaktinformationen</b>	Bitmessage-Adresse: <a href="#">BM-NB0GrABB2ShNwH0St0CzLVKDySYNvCF</a> Bitmessage-Adresse: Eine Bitmessage mittels Forum schicken. PGP-Schlüssel: <a href="#">Schlüssel anzeigen</a>
<b>Themen und Beiträge</b>	Alle Beiträge von rico anzeigen Alle Themen von rico anzeigen
<b>Aktuelle Signatur</b>	Zeit ist Geld

Deutschland im Deep Web > Profil von **rico**

# Operation Hardes

## Operation HARDES



- Nationwide operation from 04.09. – 12.09.2012
- 2 undercover agents pretending to be 13y old girls



# Operation Hardes

**Knuddels.de**

1<vivi>    yannik1994

**Kostenlos registrieren**

Alter: 12 ✓ männlich ✓  
 Nickname: BerndBrot ✓  
 Passwort: ..... ✓  
 E-Mail: berndbrot@daserste.de

Ich akzeptiere hiermit die [AGB](#) und [Datenschutzrichtlinien](#).

**Registrieren und Loslegen!**

Flirt: 2962    Over 20: 1361    Under 18: 8

Games: 876    Card Games: 1000    Themetalk: 696    Top MyChannels: 1561

Werde Knuddels-Fan auf Facebook!

88.822 Fans   

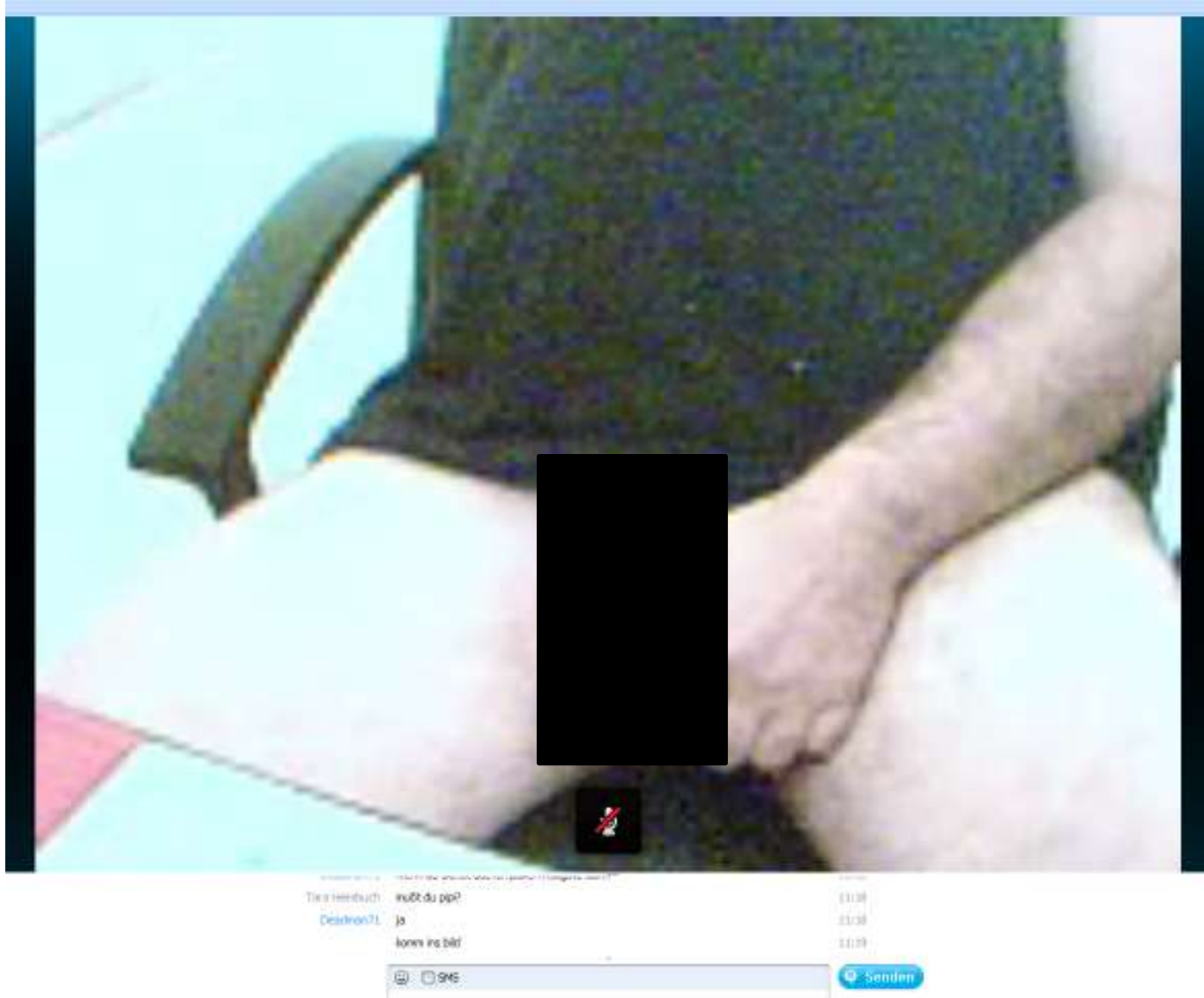
1.178 benötigte Fans für Knuddels

SALE %    % SALE %    %

AKTUELLE KOLLEKTION HERBST WINTER

**BRAX**

## Operation HARDES - Example





# Results

Jana Schneider	zeig dich	16:13
<div style="border: 1px solid #ccc; padding: 5px; margin: 5px 0;"> <span style="font-size: 1.2em;">📞</span> Anruf von <b>Jana Schneider</b> </div>		16:13
Jana Schneider	seh dich nicht	16:14
Tara Heimbuch	ich seh dih auch net	16:14
Jana Schneider	nur, ich kill dein pc wenn ich dich nicht gleich sehe	16:14
	also mach an	16:14
	letzte chance	16:15
	zeig dich	16:15
	ok, du willst es nicht anders. mach was ich will, oder dein pc ist schrott, und alle pc´s von deine skype freunden werden infiziert	16:16
	ok, du willst es nicht anders. mach was ich will, oder dein pc ist schrott, und alle pc´s von deine skype freunden werden infiziert	16:16
	habe sämtliche daten von deinem pc kopiert	16:16
	machst du alles was ich will?	16:16
Tara Heimbuch	du machst mir angst. wer bistb du	16:16



# Results

Jana Schneider	bist du irgendwie dumm, ich habe keine webcam	16:20
Tara Heimbuch	du lügst	16:20
Jana Schneider	wenn du dich nicht in 10 sekunden zeigst, ist dein pc kaputt	16:20
	10	16:20
	9	16:20
	8	16:20
	7	16:20
	6	16:20
	5	16:20
	4	16:21
	3	16:21
	2	16:21
	1	16:21

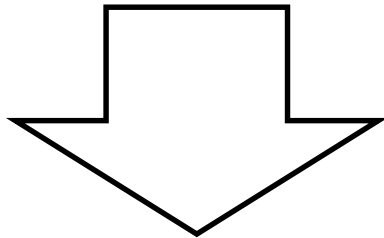
## Results

- Time-frame: 7 days
- 395 advances by pedophiles
- Sexual activity (e.g. masturbation) in front of webcam in 39 cases
- Transmission of child pornography in 5 cases
- Coordinated execution of search warrants in Feb. 2013



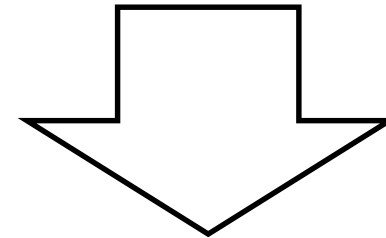
# (Undercover) investigation-methods in Germany

Technical Approach



Wiretapping, Data-traffic-interception, information requests (content data, metadata, subscriber data), GPS-trackers, use of IP-trackers (tools to track the real ip-address)

Standard investigations



„Traditional“ undercover work, surveillance, observations, undercover agents, informants, mock purchases (pseudo buys)



## What we still may not do under German procedural laws

Unfortunately it is still not allowed to

- covertly search external IT-devices by online remote access (e.g. by a RAT)
- covertly seize data stored on external IT-systems (the general procedural provisions for seizures still apply, but by resorting to them the affected person must be notified after the measure is carried out)

# IP-tracking

„IP-tracking“ ...

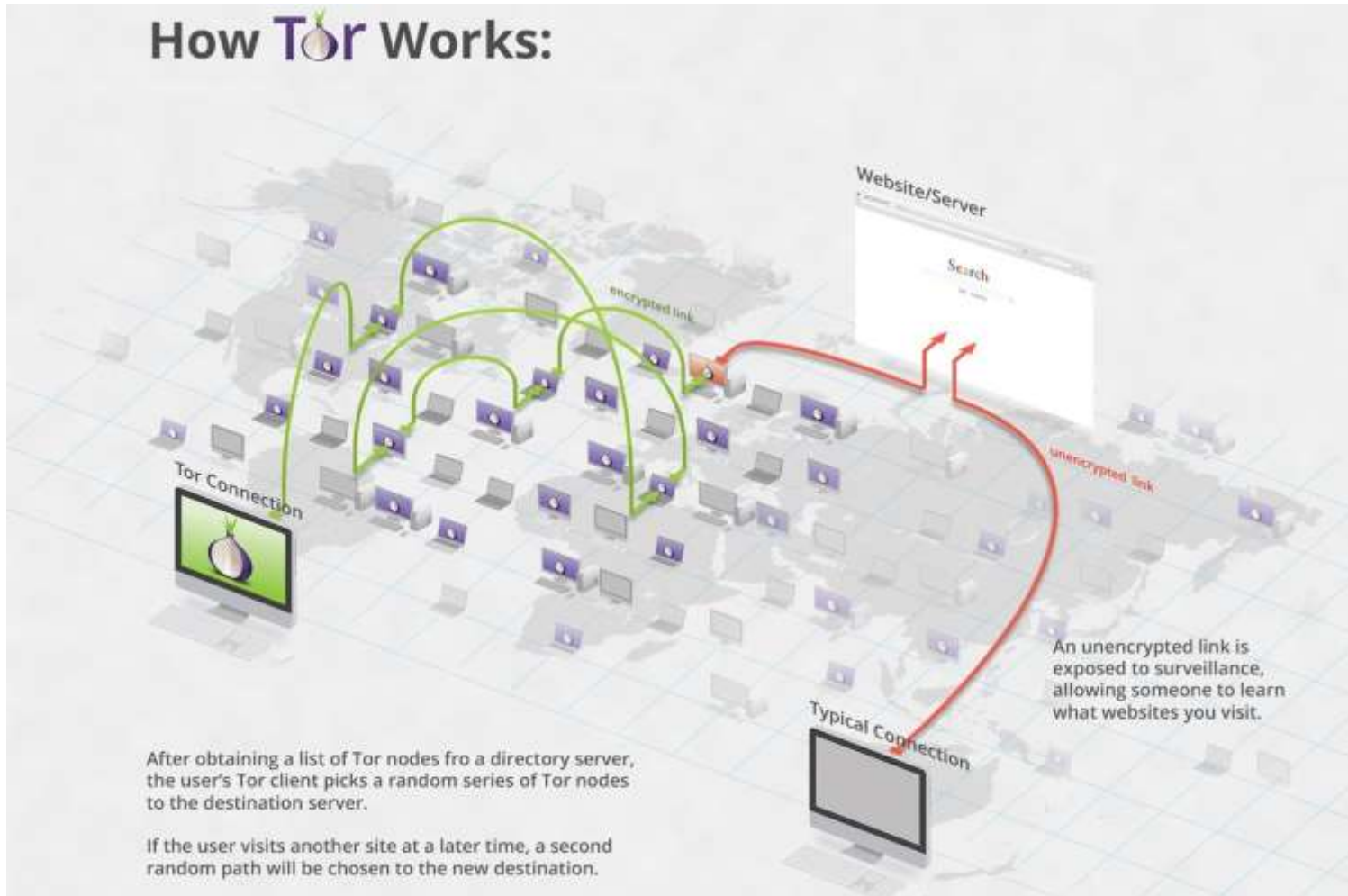
What does that mean?

Why is that necessary?

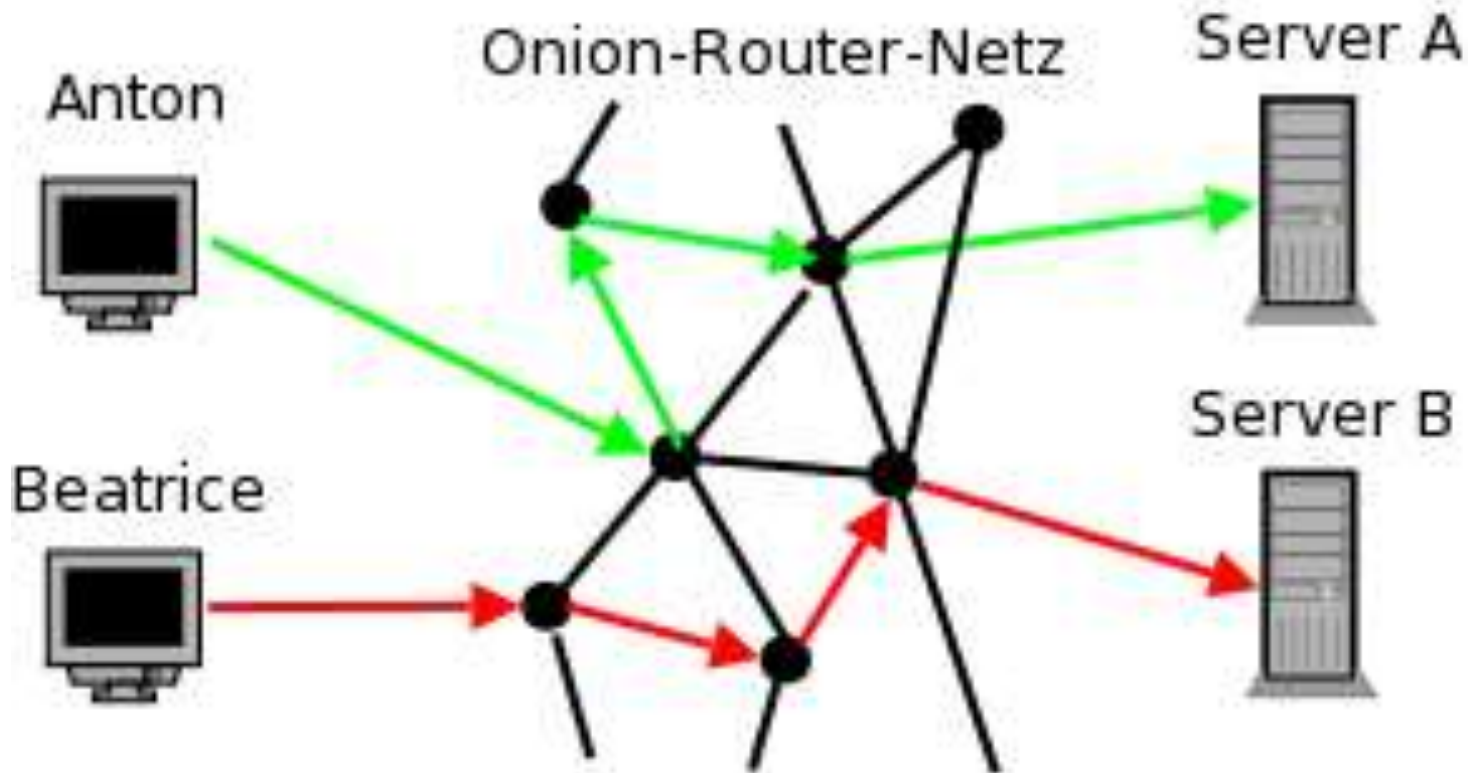
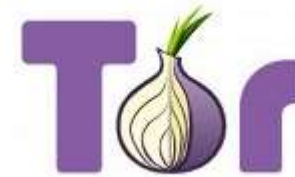


# Darknet

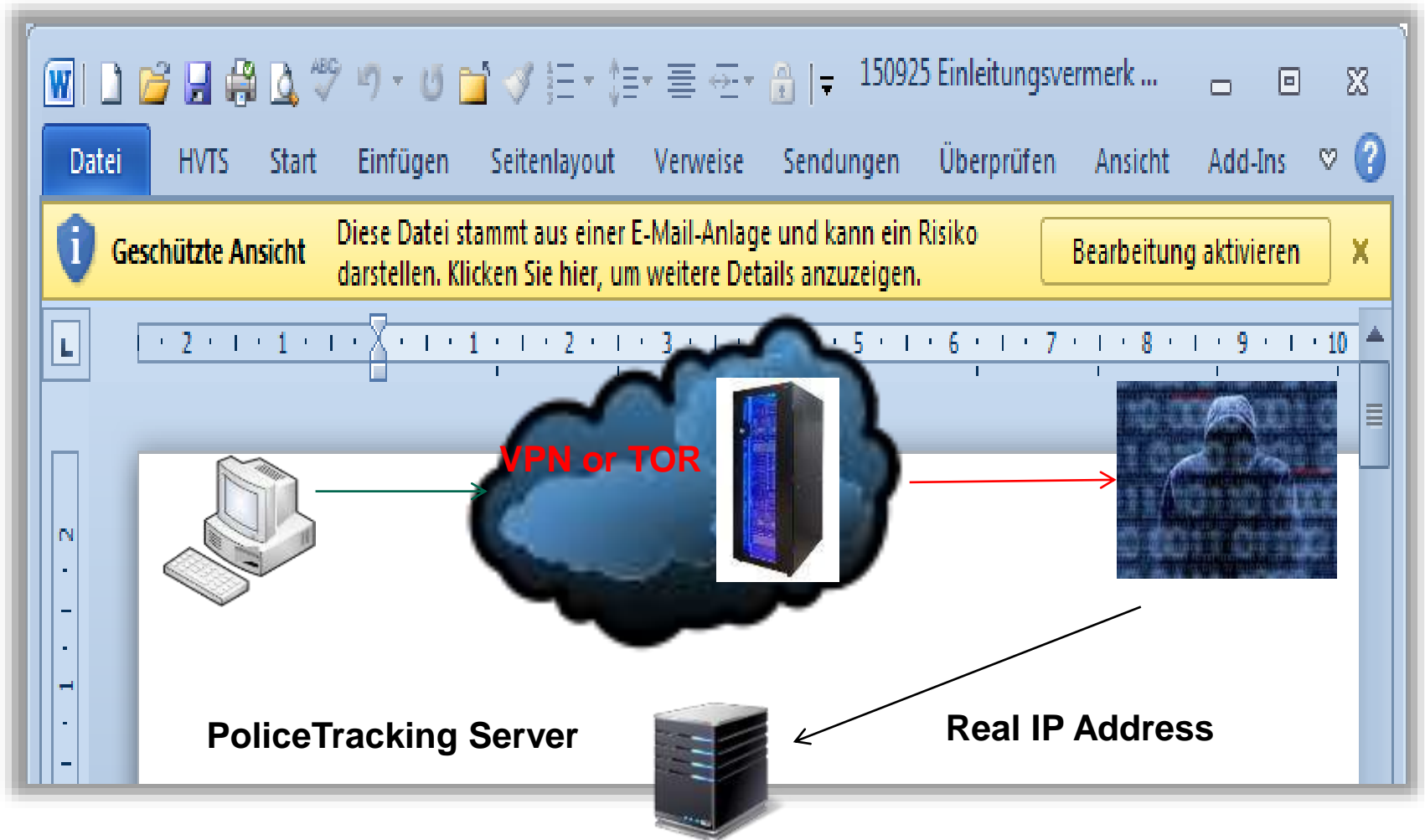
## How Tor Works:



# The Onion Router (TOR) software as a tool for anonymization and encryption of TC



# IP-tracking-tools



## Practical Experiences – what’s not feasible?

### Subscriber-data requests to providers?

(§§ 100j StPO / §§ 14, 15 TMG i.V.m. 161 StPO)

- Platform-operators usually are non-cooperative
- Production orders and data requests can’t be legally enforced

### Financial-investigations in the Darknet?

(§§ 161, 161a, 163 StPO)

- Since there are no banks involved, no requests for account-data
- Bitcoins are „anonymous“

## Practical Experiences – what's not feasible?

### Seizure of servers?

(§§ 94, 95, 98 StPO)

- Host-provider aren't traceable within the Darknet

### Wiretapping/ Server-traffic-interception?

(§§ 100a, 100b StPO)

- ISPs of customers/owners/operators of platforms are unknown
- When using TOR, wiretapping only reveals encrypted traffic-data

## Practical Experiences – what's feasible?

### Faked communication with vendor

(§§ 161, 163 StPO)

- Set up account by using fake-ID
- What does the vendor tell about him?

### Mock-purchases of guns, drugs, counterfeit etc.

(§§ 161, 163 StPO)

- Examination of delivered items/ confirmation of suspicion
- Examination of trace material (package etc.)
- Identification through fingerprints/DNA?



## Practical Experiences – what’s feasible?

### Faked communication with vendor

(§§ 161, 163 StPO)

- Set up account by using fake-ID
- What does the vendor tell about...

### Mock-purchase

**Regularly unsuccessful!**

...for delivered items/ confirmation of suspicion  
 Examination of trace material (package etc.)

- Identification through fingerprints/DNA?

## Practical Experiences – what’s feasible?

### Faked communication with vendor

(§§ 161, 163 StPO)

- PGP-encrypted communication (email identifiable?)
- „Negotiations“ supported through pics sent (IP-tracking, meta-data)?
- Pics to be shared with counterpart uploaded to cloud (requests for user-data filed with providers)?

### Mock-purchases of guns, drugs, counterfeit etc.

(§§ 161, 163 StPO)

- Tracing of package by tracking-numbers, parcel-stamp, drop-stations
- Cooperation with carriers (DHL)
- Parcel-seizure; observation at drop-stations





Any questions?

Office of the Attorney General of the federal state of Hesse  
email: [ZIT@GStA.Justiz.Hessen.de](mailto:ZIT@GStA.Justiz.Hessen.de)