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 Hessia – 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
The ages of the digital revolution

World Internet Usage Growth

million persons

0 16 35 70 147 248 361 513 587 719 817 1,018 1,093 1,319 1,574 1,802 1,971 2,267 2,497 2,749

The actual relevance of cybercrime is only insufficiently displayed in official statistics, real numbers remain largely unclear.
Estimations by the internet-industry

**SHOCKING SCALE: NUMBER OF VICTIMS**

*1 MILLION+ VICTIMS A DAY*

Every day there are twice as many cybercrime victims as newborn babies.

- **50,000** victims every hour
- **820** victims every minute
- **14** victims every second

**THE SHOCKING SCALE OF CYBERCRIME**

*$388 BILLION*

The total bill for cybercrime footed by online adults in 24 countries topped USD $388bn over the past year.

- **$114bn**
- **$274bn**

Victims valued the time they lost to cybercrime at over...
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

- **Supervising authority**
  - Coordination
  - Training
  - Contact point
  - Support/ crime-prevention

- **Prosecuting authority**
  - Running cases and conducting investigations of particular importance and difficulty
  - International Coordination (in transnational cases)
  - Expedited measures / procedures
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 aquisition 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
Requirements
Tor-Browser

Willkommen im Tor Browser
Sie können jetzt anonym im Internet surfen.

Tor-Netzwerkeinstellungen testen

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

Willkommen im Tor Browser

grams7enufi7jmdl.onion/
Search the darknet

Heroin

Grams Search  I'm Feeling Lucky
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
Drugs, drugs, drugs...
...and even more drugs
Firearms

Search the darknet

Glock

Grams Search  I'm Feeling Lucky
Firearms
...all roads lead to AlphaBay
Thus, the place to be for Organized Arms-traffickers
Trade in counterfeit
Trade in forged official documents

<table>
<thead>
<tr>
<th>Price</th>
<th>119,23066 BTC</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>$ 1,279.50</td>
</tr>
<tr>
<td></td>
<td>£ 800.89</td>
</tr>
<tr>
<td></td>
<td>€ 1,000.00</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Ship from</th>
<th>Germany</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ship to</td>
<td>worldwide</td>
</tr>
<tr>
<td>Stock</td>
<td>100</td>
</tr>
<tr>
<td>Created in</td>
<td>2012-11-01 15:58 UTC</td>
</tr>
<tr>
<td>Last update</td>
<td>2012-11-03 11:19 UTC</td>
</tr>
</tbody>
</table>

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/recvie 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

Webserver
Keine Bekanntheit, so wie 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, so wie 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, so wie 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 hat, dieser jedoch nach 1 Stunde eine neue IP hat (vgl. dynamisch) muss 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 IPs gleichzeitig gehielt 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 - 3:00

§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 xxx@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

Screenshot of an email discussing the sale of a database containing 11 million UK date of birth (DOB) records for $25,000. The email contains a sample of the database and details on the price and terms of sale. It also mentions the possibility of creating a custom search service for $1,000.
Mechanisms of darknet-markets: The rating-systems

<table>
<thead>
<tr>
<th>From</th>
<th>Rate</th>
<th>User As</th>
<th>Message</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>theduke71</td>
<td></td>
<td>seller</td>
<td>Goods as advertised and a nice guy</td>
<td>(´• 5x Party Flock (purple)...)</td>
</tr>
<tr>
<td>rizia</td>
<td></td>
<td>seller</td>
<td>Ok, all good.. S/S thanks bro...</td>
<td>(´• 1x Party Flock (purple)...</td>
</tr>
<tr>
<td>experience2080</td>
<td></td>
<td>seller</td>
<td>Excellent, fast shipping. Thanks</td>
<td>(´• 1.0gr Very Pure Cocaine...</td>
</tr>
<tr>
<td>justjohn</td>
<td></td>
<td>seller</td>
<td>good seller, good delivery</td>
<td>(´Very Pure Cocaine 80% ...</td>
</tr>
<tr>
<td>pindulinka</td>
<td></td>
<td>seller</td>
<td>Arrived and I am happy, satisfied, thanks A+</td>
<td>(´Very Pure Cocaine 80% ...</td>
</tr>
<tr>
<td>13White_Widow37</td>
<td></td>
<td>seller</td>
<td>He Sent at Friday and I received it Wednesday. Really good Product! Recommended for MDMA and Fill Lovers :)</td>
<td>(´1 x Party Flock (purple)...</td>
</tr>
<tr>
<td>freedani88</td>
<td></td>
<td>seller</td>
<td>thnx :D</td>
<td>(´10x 20 euro notes COUN...</td>
</tr>
<tr>
<td>cardolastk</td>
<td></td>
<td>seller</td>
<td>good bro, honest seller!</td>
<td>('SpyEye Botnet v.1.34B...</td>
</tr>
<tr>
<td>maarten0</td>
<td></td>
<td>seller</td>
<td>nice stuff ;-) - thank you;)</td>
<td>(´0.5gr Very Pure Cocaine...</td>
</tr>
<tr>
<td>gaumeland</td>
<td></td>
<td>seller</td>
<td>Very nice sample of real cocaine...</td>
<td>(´Very Pure Cocaine 80% ...</td>
</tr>
</tbody>
</table>
Mechanisms: The delivery of purchased goods
Mechanisms of the darknet-markets: The payment
Mechanisms of the darknet-markets: The payment
CryptoLocker

Your personal files are encrypted!

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 RSA-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.

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

Time left
56 : 16 : 12
Cybercrime and „Underground Economy“

OP Onymous
OP Onymous

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

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

The 7 signs of infection:

- **Mouse**
  - cursor moves erratically

- **Webcam**
  - light unexpectedly turns on

- **Monitor**
  - turns off while in use

- **Passwords**
  - online accounts have been compromised

- **Money**
  - unauthorized login to bank accounts

- **Chat**
  - chat windows appear unexpectedly

- **Ransom**
  - ransom demand is made to unlock files

Learn more at:
www.stateoftheinternet.com/blackshades
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 a video.

Quality at 100

Quality at 50
### TOP 5 COUNTRIES AFFECTED BY BLACKSHADES 2013/2014

<table>
<thead>
<tr>
<th>Country</th>
<th>Affected %</th>
</tr>
</thead>
<tbody>
<tr>
<td>US</td>
<td>37%</td>
</tr>
<tr>
<td>Germany</td>
<td>13%</td>
</tr>
<tr>
<td>UK</td>
<td>9%</td>
</tr>
<tr>
<td>Netherlands</td>
<td>9%</td>
</tr>
<tr>
<td>France</td>
<td>8%</td>
</tr>
</tbody>
</table>

Majority of infections are in the US and Europe.

@threatintel | www.symantec.com
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“)
„Bitcoin-Mining“

- **But:** Mining on a standard computer takes years

- Costs for electric power used by the computer exceed 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
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
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

MÜNCHEN

Olympia-Einkaufszentrum (OEZ)
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

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.
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“
Operation Hardes
Operation HARDES

• Nationwide operation from 04.09. – 12.09.2012

• 2 undercover agents pretending to be 13y old girls
Operation Hardes
Operation HARDES - Example
<table>
<thead>
<tr>
<th>Zeit</th>
<th>Benutzer</th>
<th>Nachricht</th>
</tr>
</thead>
<tbody>
<tr>
<td>16:13</td>
<td>Jana Schneider</td>
<td>zeig dich</td>
</tr>
<tr>
<td>16:13</td>
<td>Anruf von Jana Schneider</td>
<td>Anruf von Jana Schneider</td>
</tr>
<tr>
<td>16:14</td>
<td>Jana Schneider</td>
<td>seh dich nicht</td>
</tr>
<tr>
<td>16:14</td>
<td>Tara Heimbuch</td>
<td>ich seh dich auch net</td>
</tr>
<tr>
<td>16:14</td>
<td>Jana Schneider</td>
<td>nur, ich kill dein pc wenn ich dich nicht gleich sehe</td>
</tr>
<tr>
<td></td>
<td></td>
<td>also mach an</td>
</tr>
<tr>
<td></td>
<td></td>
<td>letzte chance</td>
</tr>
<tr>
<td></td>
<td></td>
<td>zeig dich</td>
</tr>
<tr>
<td></td>
<td></td>
<td>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</td>
</tr>
<tr>
<td></td>
<td></td>
<td>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</td>
</tr>
<tr>
<td></td>
<td></td>
<td>habe sämtliche Daten von deinem pc kopiert</td>
</tr>
<tr>
<td></td>
<td></td>
<td>machst du alles was ich will?</td>
</tr>
<tr>
<td></td>
<td>Tara Heimbuch</td>
<td>du machst mir angst. wer bistb du</td>
</tr>
<tr>
<td>Name</td>
<td>Message</td>
<td>Time</td>
</tr>
<tr>
<td>---------------------</td>
<td>-------------------------------------------------------------------------</td>
<td>-------</td>
</tr>
<tr>
<td>Jana Schneider</td>
<td>bist du irgendwie dumm, ich habe keine webcam</td>
<td>16:20</td>
</tr>
<tr>
<td>Tara Heimbuch</td>
<td>du lügst</td>
<td>16:20</td>
</tr>
<tr>
<td>Jana Schneider</td>
<td>wenn du dich nicht in 10 sekunden zeigst, ist dein pc kaputt</td>
<td>16:20</td>
</tr>
<tr>
<td></td>
<td>10</td>
<td>16:20</td>
</tr>
<tr>
<td></td>
<td>9</td>
<td>16:20</td>
</tr>
<tr>
<td></td>
<td>8</td>
<td>16:20</td>
</tr>
<tr>
<td></td>
<td>7</td>
<td>16:20</td>
</tr>
<tr>
<td></td>
<td>6</td>
<td>16:20</td>
</tr>
<tr>
<td></td>
<td>5</td>
<td>16:20</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>16:21</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>16:21</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>16:21</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>16:21</td>
</tr>
</tbody>
</table>
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 neccessary?
After obtaining a list of Tor nodes from a directory server, the user’s Tor client picks a random series of Tor nodes to the destination server.

If the user visits another site at a later time, a second random path will be chosen to the new destination.
The Onion Router (TOR) software as a tool for anonymization and encryption of TC
IP-tracking-tools

VPN or TOR

PoliceTracking Server

Real IP Address
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 him?

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

Regularity unsuccessful!
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 Hessia
email: ZIT@GStA.Justiz.Hessen.de