Dark Web

Introduction
Introduction

Allow myself to introduce...
What is the INTERNET?

- **Wikipedia**: The global system of interconnected computer networks that use the Internet protocol suite (TCP/IP) to link devices worldwide.

- **Google**: A global computer network providing a variety of information and communication facilities, consisting of interconnected networks using standardized communication protocols.

- **Cambridge Dictionary**: The large system of connected computers around the world that allows people to share information and communicate with each other.
What is the INTERNET?

• **My family:** electronic mail, world wide web, messenger, communication tool

• **My colleagues:** network of the networks, ultimate source of porn, cute pictures and videos of cats

• **My friends:** virtual network, best solution for connections and information flow, free contact and messenger, the murderer of my friends favorite porn video rental shop
The Internet how we know...

- **Crawling**: When Google visits a website for tracking purposes. This process is done by Google’s Spider crawlers.

- **Indexing**: After crawling has been done, the results get put onto Google’s index (i.e. the web search).

- If something cannot be found with Google, it does not exist.
- Is it true or false?
Exploring The Hidden Internet

Surface Web

Deep Web
- Legal Documents
- Government Records
- Scientific Reports
- Academic Records
- Financial Records

Dark Web
- Drugs
- Tor
- Illegal Info
The Deep Web

- **The Deep Web** (invisible web or hidden web) is part of the World Wide Web but the contents are not indexed by standard web search engines for any reason.

- For example:
  - Password protected
  - Contains file types which are not indexed by crawlers
  - Can be reached only with specific DARKNET software
The Darknet

- **The Darknet**: An encrypted network built on top of the existing Internet, and specific software or tools are required to access it. Darknet provides anonymity to the users. Darknet is for example TOR, Freenet or I2P.
The Dark Web

- **The Dark Web** is the World Wide Web content that exists on Darknets and requires specific software, configurations, or authorization to access.
The TOR Network

• was developed in the mid-1990s by US Naval Research Laboratory
• special proxy network (client – node – tor-exit)
• daily users average 2 000 000 Worldwide (650 in Albania, 1250 in Slovenia, 4000 in Hungary, 400 000 in USA)
• Requires a special browser (TOR Browser)
• Free to download it, legal to use it
• Special domains .onion, but „normal” websites can be open with it
TOR: STRENGTH IN NUMBERS

Advance universal human rights. Protect the privacy of millions. Your financial support will allow people around the world to be more safe online.

Give today, and Mozilla will match your donation.

Count me in

We're hiring! »

Recent Blog Posts

New Release: Tor Browser for And...
Wed, 31 Oct 2018  
Posted by: syarqo

New Release: Tor Browser 8.5.4
Tue, 23 Oct 2018  
Posted by: boekim
# The TOR Project

## Our Projects

<table>
<thead>
<tr>
<th>Project</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tor Browser</td>
<td>Tor Browser contains everything you need to safely browse the Internet.</td>
</tr>
<tr>
<td>Orbot</td>
<td>Tor for Google Android devices.</td>
</tr>
<tr>
<td>Tails</td>
<td>Live CD/USB operating system preconfigured to use Tor safely.</td>
</tr>
<tr>
<td>Nyx</td>
<td>Terminal (command line) application for monitoring and configuring Tor.</td>
</tr>
<tr>
<td>Relay Search</td>
<td>Site providing an overview of the Tor network.</td>
</tr>
<tr>
<td>Pluggable Transports</td>
<td>Pluggable transports help you circumvent censorship.</td>
</tr>
<tr>
<td>Stem</td>
<td>Library for writing scripts and applications that interact with Tor.</td>
</tr>
<tr>
<td>OONI</td>
<td>Global observatory monitoring for network censorship.</td>
</tr>
</tbody>
</table>

Learn more about our projects »
The TOR Circuit

- Tor client
- Entry guard
- Middle relay
- Exit relay
- Tor network
- Destination

- Encrypted by Tor
- Not encrypted by Tor
The TOR Encryption

Source

Router A

Router B

Router C

Message

Destination
This slide cannot be disclosed due to public security
This slide cannot be disclosed due to public security
This slide cannot be disclosed due to public security
This slide cannot be disclosed due to public security
What are the disadvantages?

• It is for anonymity and not for encryption
• Slow connection speed
• Sometimes the network is unstable
• Some websites denying TOR exit nodes (as disallowed IPs)

Access Denied

You don't have permission to access "http://www.footlocker.com/" on this server.

Reference #18.9e3919b8.1541199237.20499dd
how do i get to the...
Let’s find some Dark Web URLs... but on the Surface Web...

- http://www.deepdotweb.com/
- http://darkwebnews.com/dark-web-market-list/
- https://dnstats.net/#
- http://darknetmarkets.org/
- http://www.gvibes4u.com/list-of-darknet-marketplaces-pages/
- http://thehiddenwiki.org/
What can we find on the Dark Web?

- **Legal** 47.7%
- **Site Down** 17.7%
- **Drugs** 12.3%
- **Explicit** 6.5%
- **Multiple Categories (Illicit)**
  - Pharmaceuticals 3.2%
  - Other Illicit Activity 1.5%
  - Hacking & Exploits 1.3%
  - Fraud 1.3%
  - Exploitation 1.0%
  - Downloadable 0.5%
  - Extremism 0.2%

CEPOL
The (uncensored) Hidden Wiki

Welcome to The Hidden Wiki. New hidden wiki url 2018 http://zqktlw4f3ecv06rl.onion Add it to bookmarks and spread it!!!!

Editor's picks

Pick a random page from the article index and replace one of these slots with it:
1. The Matrix - Very nice to read.
2. How to Exit the Matrix - Learn how to Protect yourself and your rights, online and off.
5. Terrific Strategies To Apply A Social media Marketing Approach - Great tips for the internet marketer.

Volunteer

Here are the six different things that you can help us out with:
1. Plunder other hidden service lists for links and place them here!
2. File the SnapBBSIndex links wherever they go.
3. Set external links to HTTPS where available, good certificate, and same content.
5. Perform Dead Services Duties.
6. Remove CP shitness.

Introduction Points

- Ahnya $ - Clearet search engine for Tor Hidden Services
- DuckDuckGo $ - A Hidden Service that searches the clearenet
- TorLinks $ - TorLinks is a moderated replacement for The Hidden Wiki.
- Torch $ - A Tor Search Engine. Claims to index around 1.1 Million pages.
- The Hidden Wiki $ - A mirror of the Hidden Wiki. 2 days old users can edit the main page. [redirect]
Marketplaces

- New generation of vendors and buyers, everybody keeps anonymity
- The first marketplace was opened in 2011 (Silk Road)
- General currency is Bitcoin or other cryptocurrencies
- There are general marketplaces and special ones only for one or two type of goods
- Despite law enforcement counter measures (Silk Road, AlphaBay, Hansa, etc.) it is a rapidly growing business
- The biggest now days are Dream Market, The Wall Street Market, Point/Tochka Free Market
Marketplaces – How they operate?

• Only username and password needed (no e-mail, no phonenumber, no credit card number, no real personal data)
• Sometimes Vendor status requires a bond of app. $0.1 ($634)
• There is escrow protection
• Forum, Chat rooms, Bug hunting for money

How the Marketplace works
Marketplaces – What can we buy?

- All type of drugs
- Medicine
- Steroids
- Counterfeited money
- Forged documents
- Fake bank statement
- Payment card data
- Bank account data
- Child abuse material
- Prostitutes
- Hitman
- Hacking activity
- Stolen goods
- Weapons, ammo
- Guidelines
This slide cannot be disclosed due to public security.
This slide cannot be disclosed due to public security
This slide cannot be disclosed due to public security.
This slide cannot be disclosed due to public security
This slide cannot be disclosed due to public security
This slide cannot be disclosed due to public security
This slide cannot be disclosed due to public security
This slide cannot be disclosed due to public security
This slide cannot be disclosed due to public security
This slide cannot be disclosed due to public security
This slide cannot be disclosed due to public security
This slide cannot be disclosed due to public security
This slide cannot be disclosed due to public security
This slide cannot be disclosed due to public security
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
This slide cannot be disclosed due to public security
**MASSIVE BLOW TO CRIMINAL DARK WEB ACTIVITIES AFTER GLOBALLY COORDINATED OPERATION**

20 July 2017

**Press Release**

Takedown of AlphaBay and Hansa will lead to hundreds of new investigations in Europe

Months of preparation and coordination have resulted today, 20 July 2017, in the takedown of two of the largest criminal Dark Web markets, AlphaBay and Hansa.
So let’s continue taking down the bad guys...
Thank you for your attention!
International Cooperation

Digital evidences abroad
Introduction

Allow myself to introduce...
Key findings

• Digital globalization
• Cloud computing
• Criminals and crimes become more transnational
• No borders for criminals
• Borders for law enforcement
• Legal regulations changing very slow
• Law enforcement and judicial authorities hardly adapt
Some problems...

- Phone numbers
- E-mail address
- IP addresses
- Data storage
- Bank accounts
- Property
- Other financial actions
Convention on Cybercrime („Budapest Convention”)  

- drawn up by the Council of Europe in Strasbourg  
- signed in Budapest 23/11/2001  
- open for signature by the member States and the non-member States (61 ratifications now)  
- the main objective is a common criminal policy for the protection of society against cybercrime  
- the first international treaty on crimes committed via the Internet (infringements of copyright, computer-related fraud, child pornography, violations of network security)  
- it also contains a series of powers and procedures
Convention on Cybercrime („Budapest Convention”)

- **preservation** of stored data, preservation and partial disclosure of traffic data, production order, **search and seizure** of computer data, real-time **collection** of traffic data, and **interception** of content data.

- contains a provision on a specific type of **trans border access** to stored computer data which does not require mutual assistance (with consent or where publicly available)

- provides for the setting up of a **24/7 network** for ensuring speedy assistance among the Signatory Parties.
Why this is important for us?

• Preamble: ...and to enable the collection of evidence in electronic form of a criminal offence;

• Article 14: ...each Party shall apply the powers and procedures referred to in paragraph 1 of this article to: ...c the collection of evidence in electronic form of a criminal offence

• Article 25: The Parties shall afford one another mutual assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.
This slide cannot be disclosed due to public security
This slide cannot be disclosed due to public security
This slide cannot be disclosed due to public security.
Other 24/7 channels

• **G7 network** (Established by G7 Subgroup on High-Tech Crime in 1998, 71 members, updated by USA Department of Justice – Albania has a PoC)

• **INTERPOL DIGITAL CRIME CENTER 24/7** (Established by INTERPOL, almost 200 members, updated by INTERPOL – Albania has a PoC)
This slide cannot be disclosed due to public security
Why is it good and how can we use it?

- Fast, direct, electronic channel
- English speaking police officers
- Ask for information (legal requirement, competent authority, general practice, contact info, etc.)
- Ask for preservation of stored data and traffic data, production order, search and seizure of computer data, real-time collection of traffic data, interception of content data
This slide cannot be disclosed due to public security
Thank you for your attention!

European Union Agency for Law Enforcement Training
Offices: H-1066 Budapest, Ö utca 27., Hungary • Correspondence: H-1903 Budapest, Pf. 314, Hungary
Telephone: +36 1 803 8030 • Fax: +36 1 803 8032 • E-mail: info@cepol.europa.eu •
www.cepol.europa.eu
What is OSINT?

• Open Source Intelligence: an intelligence gathering method which involves finding data in sources publicly and legally available for everyone and analyzing it to be used in an intelligence context

Digital footprint

• Every action on the Internet leaves a trace behind
• At least an username, an e-mail account and a password is necessary almost everywhere
• Once it is there, it can be only hardly or never removed...
Intelligence gathering methods

- HUMINT – Human Intelligence
- MASINT – Measurement and Signature Intelligence
- GEOINT – Geospatial Intelligence
- SIGINT – Signals Intelligence
- TECHINT – Technical Intelligence
- MARKINT – Market Intelligence
- OSINT – Open Source Intelligence
- Etc.

OSINT vs. other intelligence gathering methods

- In other intelligence methods the hardest part is obtaining the data while in OSINT the major difficulty is to analyze and verify it.
- It became essential after the Internet explosion
- 90% of data processed by intelligence services is based on open sources
OSINT vs. other intelligence gathering methods

- **Advantages:**
  - Easy to access
  - Cheap or free
  - Big volume of data
  - Good chance to get information
  - Can be used without permission
  - Open sources usually record historical data too

- **Disadvantages:**
  - Time consuming
  - Needs new type of skills and knowledge
  - Big volume of data
  - Many fake information, reliability of data
  - You need other sources for verifying

---

OSINT Methods

- **Passive:** no interaction with the target
  
  „The quieter you become the more you are able to hear.”
  
  (Ram Dass)

- **Active:** taking some intrusive steps is necessary to get the information (e.g. follow an Instagram profile, send a friend request or join a group on FB, etc.)
  
  „The line between ACTIVE OSINT and HACKING is very thin.”
  
  (Anybody who teaches OSINT)
Open sources

- Media: newspapers, magazines, radio, television...
- Public databases: libraries, universities, governmental bodies, NGOs, research facilities, private companies...
- Publications: governmental reports, studies, academic papers...
- Public conferences and other public events...
- World Wide Web

Why is the internet is the most important source?

- Easy to access
- Used by everyone – including criminals
- Timeless and timely
- The quantity of the data on the world wide web grows exponentially
- Contains everything mentioned before and a lot more
- There are types of data which could be obtained only from the web
Exponential growth in the last two decades

<table>
<thead>
<tr>
<th>Year</th>
<th>Internet Users**</th>
<th>Penetration (% of Pop)</th>
</tr>
</thead>
<tbody>
<tr>
<td>2016</td>
<td>3,424,971,237</td>
<td>46.1 %</td>
</tr>
<tr>
<td>2015</td>
<td>3,185,996,155</td>
<td>43.4 %</td>
</tr>
<tr>
<td>2014</td>
<td>2,996,385,869</td>
<td>40.7 %</td>
</tr>
<tr>
<td>2013</td>
<td>2,728,428,107</td>
<td>38 %</td>
</tr>
<tr>
<td>2012</td>
<td>2,494,736,248</td>
<td>35.1 %</td>
</tr>
<tr>
<td>2011</td>
<td>2,311,957,359</td>
<td>31.8 %</td>
</tr>
<tr>
<td>2010</td>
<td>2,022,620,974</td>
<td>29.2 %</td>
</tr>
<tr>
<td>2009</td>
<td>1,766,483,814</td>
<td>25.8 %</td>
</tr>
<tr>
<td>2008</td>
<td>1,575,067,520</td>
<td>23.3 %</td>
</tr>
<tr>
<td>2007</td>
<td>1,373,226,988</td>
<td>20.6 %</td>
</tr>
</tbody>
</table>

GLOBAL DIGITAL SNAPSHOT
THE EFFECT ONERS FOR INTERNET, SOCIAL MEDIA, AND MOBILE USAGE AROUND THE WORLD

- **TOTAL POPULATION**
  - 7.497 BILLION
  - URBANIZATION: 54%
  - PENETRATION: 66%

- **INTERNET USERS**
  - 3.811 BILLION
  - PENETRATION: 51%

- **ACTIVE SOCIAL MEDIA USERS**
  - 2.907 BILLION
  - PENETRATION: 39%

- **UNIQUE MOBILE USERS**
  - 4.960 BILLION
  - PENETRATION: 36%

- **ACTIVE MOBILE SOCIAL USERS**
  - 2.698 BILLION
  - PENETRATION: 36%
What are the most important sources?

- Websites
- Search engines
- Online databases
- Instant message apps
- Maps
- Photos, videos
- Dark web
- Social media

Internet Users in the world: 3,757,261,687
Total number of Websites: 1,273,496,747
Emails sent today: 132,610,427,629
Blog posts written today: 2,870,676
Tweets sent today: 377,610,348
Google searches today: 3,059,114,974
Websites

- Websites made by the suspect or visited by the suspect can contain useful information
- Website vs. Webpage
- **Tip:** a comment section of a website is a good source
- **Tool:** for downloading a website use Httrack (https://www.httrack.com)
Search engines

- The BIG ONES: Google, Bing (Yahoo), Yandex (Russia), Baidu (China)
- Special search engines:
  - Country based search engines
  - People search engines
  - Social media search engines
  - Deep web search tools
  - Etc.
- **Tip:** always check Bing also
- **Tool:** use Google Search Operators and Google Advanced Search
<table>
<thead>
<tr>
<th>GOOGLE Search Operator</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>allinurl: / inurl:</td>
<td>Pages containing keywords in:</td>
</tr>
<tr>
<td>allintitle: / intitle:</td>
<td>- the URL</td>
</tr>
<tr>
<td>allintext: / intext:</td>
<td>- the Title</td>
</tr>
<tr>
<td>cache:</td>
<td>- cache</td>
</tr>
<tr>
<td>filetype:</td>
<td>- after the last period in file name</td>
</tr>
<tr>
<td>site:</td>
<td>Narrow results to a site</td>
</tr>
<tr>
<td>related:</td>
<td>Shows similar sites</td>
</tr>
<tr>
<td>info:</td>
<td>Shows page info</td>
</tr>
<tr>
<td>&quot;keyword keyword&quot;</td>
<td>Search for a phrase</td>
</tr>
<tr>
<td>-</td>
<td>Exclusion</td>
</tr>
<tr>
<td>OR</td>
<td>Alternatives</td>
</tr>
</tbody>
</table>

- Stolen Samsung laptop probably sold on www.vatera.hu
  `site:vatera.hu "samsung laptop" AND "for sale"`
- Looking for word documents on www.police.hu
  `site:police.hu filetype:doc OR filetype:docx`
- Looking for CV on www.un.org
Online Databases

- Company registers: Information about the directors, shareholders, incorporation dates, annual reports, addresses, jurisdiction, connections...
- www.opencorporates.com
- **Tip:** try free tolls before paid services
- **Tool:** European e-Justice Portal – Company Registers (all EU members, in all EU languages)

opencorporates

Search 137,109,193 companies

CEPOL

Winner Open Data Business Award 2015
**Online Databases**

- Online auction sites: E-bay, Amazon, AliExpress, Wish
- **Tip:** search on E-bay by username

---

**Online Databases**

- Phone registers: mobile service providers search pages by country OR global online search webpages
- **Tip:** search number also in Google in different ways „0036…, +36…, without country code…, etc.”
- **Tool:** register to all of the available phone register webpages and bookmark them in your browser
SyncMe

Features

Social Caller ID
The world's most advanced caller ID. Identity incoming calls, including full names, and the phone of the caller, regardless of if they are in your phone contacts.

Sync with Social Profiles

This slide cannot be disclosed due to public security
Maps

- Google Maps and Google Earth, (Bing Maps)
- We can check almost any address without going out – even in the past
- Especially useful before an arrest and a house search
- Tip: Always check the date at the left upper corner
- Tool: Google Maps Timeline
Photos, Videos

- Photos and videos made by the target, made of the target
- We can find them everywhere, we can search them
- We can analyze them and the metadata also (sometimes)
- **Tip:** check photo metadata easily with Windows, but do not forget to analyze the photo itself
- **Tool:** for downloading a video from youtube.com use https://www.onlinevideoconverter.com
This slide cannot be disclosed due to public security
Social media

- The most important source, the backbone of every OSINT investigation
- We can obtain the most personal and up to date information about a target
- Nearly everybody was, is, or will be on some kind of a social media site
- **Tip:** check all the popular social media websites in your country
- **Tools:** we need another week for that... but let's try
Most popular social networks worldwide of (October 2018 - in millions)

- Facebook: 2,254 million
- YouTube: 1,500 million
- WhatsApp: 1,000 million
- Facebook Messenger: 1,000 million
- WeChat: 1,000 million
- Instagram: 800 million
- QZone: 800 million
- TikTok: 548 million
- Sina Weibo: 500 million
- Twitter: 350 million
- Reddit: 330 million
- LinkedIn**: 300 million
- Sina Weibo: 300 million

**Note: Data for QZone and LinkedIn is not available.
Some statistics on Facebook users

- 87% of online users of age 18-29 are on Facebook
- Half of them check Facebook when they wake up
- The average time spent on Facebook per visit is 20 minutes
- Average Facebook user has 155 friends
- Average number of pages, groups and events a user is connected to is 80

Some statistics on Facebook content

- 350 million photos uploaded every day, with 4,000 uploads per second
- Every 20 minutes, 1 million links are shared, 20 million friend requests and 3 million messages are sent
- 55 million status updates are made every day
- Every 60 seconds, 1 million comments are posted
FACEBOOK Search Bar

- Simple:
  - People who live in (places)
  - People who work at (working places)
  - People who was born in (birthplaces)
  - People who visited (visited places)
  - People who like (liked content)
  - People named (name)

- Multiplied:
  - People named XY who live in X
  - People who live in X who work at Y
FACEBOOK User ID

- What we usually need:
  - To identify the target profile
  - The name of a person is often not enough (e.g. John Smith – hundreds of results even by narrowing them down)
  - We need the user identification number ("USER_ID")

- Getting the User ID:
  - Browser add-ons
  - Collect it from the URL
  - Or from the page's source
This slide cannot be disclosed due to public security.
What is a proxy?
- A proxy server acts as an intermediary between the source and the target

What is a VPN?
- VPN stands for Virtual Private Network
- Some free solutions BUT paid are more recommended
- It masks your identity online
What is TOR?

- encrypted network that gives anonymity for the users and requires a specific software to access it
- Maybe the best solution for anonymity
What is a Virtual Machine?

- A virtual machine (VM) is a software program or operating system that exhibits the behavior of a separate computer and capable of performing tasks such as running applications and programs like a separate computer.
- Protects you and your machine
- You can simply delete it and create a new one for a new task
Thank you for your attention!