Exploring the Darknets

Stephen Heath
Partner & Advisory CISO
March 5, 2019
Darknet danger: Organs, murder, credit card info all for sale on Internet's underbelly

Medical Records For Sale in Underground Stolen From Texas Life Insurance Firm

Inside the underweb: Home to pedophiles, hitmen, drug dealers — and free speech

From drugs to killers: Exploring the Deep Web

Nyshka Chandran | @nyshkac
Surface Web

Non-indexed Sites

Government Databases

Private Forums

Anonymous Networks

Deep Web

Dark Net
Tor

“The Onion Router”
Distributed Network of relays around the world
Encrypts communications
Protects against surveillance and analysis
How Tor Works: 3

Step 3: If at a later time, the user visits another site, Alice's tor client selects a second random path. Again, green links are encrypted, red links are in the clear.
<table>
<thead>
<tr>
<th>Country</th>
<th>Mean daily users</th>
</tr>
</thead>
<tbody>
<tr>
<td>United States</td>
<td>448737 (16.13 %)</td>
</tr>
<tr>
<td>Germany</td>
<td>432813 (15.56 %)</td>
</tr>
<tr>
<td>United Arab Emirates</td>
<td>331984 (11.94 %)</td>
</tr>
<tr>
<td>Russia</td>
<td>255088 (9.17 %)</td>
</tr>
<tr>
<td>Ukraine</td>
<td>179483 (6.45 %)</td>
</tr>
<tr>
<td>France</td>
<td>121796 (4.38 %)</td>
</tr>
<tr>
<td>Netherlands</td>
<td>92432 (3.32 %)</td>
</tr>
<tr>
<td>United Kingdom</td>
<td>75602 (2.72 %)</td>
</tr>
<tr>
<td>Indonesia</td>
<td>60943 (2.19 %)</td>
</tr>
<tr>
<td>Canada</td>
<td>45921 (1.65 %)</td>
</tr>
</tbody>
</table>

Directly connecting users

The Tor Project - https://metrics.torproject.org/
Congratulations!
This browser is configured to use Tor.
You are now free to browse the Internet anonymously.
Test Tor Network Settings

What Next?
Tor is NOT all you need to browse anonymously!
You may need to change some of your browsing habits to ensure your identity stays safe.
Tips On Staying Anonymous »

You Can Help!
There are many ways you can help make the Tor Network faster and stronger:
- Run a Tor Relay Node »
- Volunteer Your Services »
- Make a Donation »

The Tor Project is a US 501(c)(3) non-profit dedicated to the research, development, and education of online anonymity and privacy. Learn more about The Tor Project »
http://3fyb44wdhnd2ghhl.onion/ – All You’re Base
http://j6im4v42ur6dpic3.onion/ – TorProject Archive
http://p3igkncehackjtib.onion/ – TorProject Media
http://kbhpodhnhfxl3clb4.onion – Tor Search
http://cipollatnumrrahd.onion/ – Cipolla 2.0 (Italian)
http://dppmfxaacucguzpc.onion/ – TorDir – One of the oldest link lists on Tor
Disclaimer

- This is the part where I start talking about criminal activity
- HIMSS actively discourages, and its employees are prohibited, from engaging in any illegal activity
- I (nor my employer/sponsors/HIMSS/etc.) do not condone this activity
- Topics discussed may be offensive to some people
- If you go on the darknet, you may see things you never wanted to see
- Do not do illegal stuff
You will never find a more wretched hive of scum and villainy.
### IP Address Information

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Country</th>
<th>Region</th>
<th>City</th>
<th>ISP</th>
</tr>
</thead>
<tbody>
<tr>
<td>67.185.98.60</td>
<td>United States</td>
<td>Washington</td>
<td>Spokane</td>
<td>Comcast Cable Communications Inc.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Continent</th>
<th>Latitude</th>
<th>Longitude</th>
<th>Time Zone</th>
</tr>
</thead>
<tbody>
<tr>
<td>North America</td>
<td>47.657</td>
<td>-117.5447</td>
<td>PST</td>
</tr>
</tbody>
</table>

Google Map for SPOKANE, WASHINGTON, UNITED STATES (New window)

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Country</th>
<th>Region</th>
<th>City</th>
<th>ISP</th>
</tr>
</thead>
<tbody>
<tr>
<td>85.25.103.119</td>
<td>Germany</td>
<td>Nordrhein-westfalen</td>
<td>Hurth</td>
<td>Plusserver Ag</td>
</tr>
</tbody>
</table>

Google Map for Hurth, Nordrhein-Westfalen, Germany (New window)
Welcome to The Hidden Wiki! New hidden wiki url 2015
http://zqktlwi4fecvo6ri.onion Add it to bookmarks and spread it!!

Editor's picks

Bored? 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.

Volunteer

Here are five 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.
4. Care to start recording onionland's history? Check out Onionland's Museum
5. Perform Dead Services Duties.

Introduction Points

Ahmia.fi - Clearnet search engine for Tor Hidden Services (allows you to add new
Contents

1 Editor's picks
2 Volunteer
3 Introduction Points
4 Financial Services
5 Commercial Services
6 Domain Services
7 Anonymity & Security
8 Hosting / Web / File / Image
9 Blogs / Essays / Wikis
10 Email / Messaging
11 Social Networks
12 Forums / Boards / Chans
13 Political Advocacy
14 Whistleblowing
   14.1 WikiLeaks
   14.2 Other
15 H/P/A/W/V/C
16 Audio - Music / Streams
17 Video - Movies / TV
18 Books
19 Drugs
20 ADULT
21 Erotica
   21.1 Noncommercial (E)
   21.2 Commercial (E)
   21.3 Animal Related
   21.4 Other
FE 1g 90% purity Coke
$85 USD / 0.377860 BTC
Vendor: Bird +99 advanced
Category: Cocaine
Ships From: Spain Ships To: Worldwide

Escrow x10 Methylphenidate XL 18mg (Concerta/Ritalin)
$70 USD / 0.311178 BTC
Vendor: mrshah +130 Verified
Category: Weed
Ships From: United Kingdom Ships To: Worldwide

Escrow 1g HIGH QUALITY indica. Free p+p. UK only
$19.08 USD / 0.084818 BTC
Vendor: Shadow +600 Verified advanced
Category: Weed
Ships From: United Kingdom Ships To: United Kingdom

FE FRESH CC/CVV FROM USA VISA/MASTER/DISCOVER Cards
$14.00 USD / 0.062235 BTC
Vendor: 609austin14 +558 advanced
Category: Money
Ships From: Unknown Anime Land Ships To: Worldwide
1g Best MDMA Crystals 84%+ Pure!

Unsere MDMA Kristalle werden von einem Holländischen Profi Chemiker hergestellt und haben die höchst mögliche Reinheit die es gibt! MDMA 84%+ EXTREME POTENT! HIGHEST ACHIEVABLE PURITY Our product is made by a pro dutch chemist with PMK oil. This is the best MDMA you can find even here, on the streets of Netherlands. It comes divided for you in small rocks, otherwise stealth being compromised. ...

Sold by DrugsFromGermany - 70 sold since Aug 16, 2015  Level 5

<table>
<thead>
<tr>
<th>Features</th>
<th>Features</th>
</tr>
</thead>
<tbody>
<tr>
<td>Product class</td>
<td>Physical package</td>
</tr>
<tr>
<td>Quantity left</td>
<td>Unlimited</td>
</tr>
<tr>
<td>Ends in</td>
<td>Never</td>
</tr>
<tr>
<td>Origin country</td>
<td>Germany</td>
</tr>
<tr>
<td>Ships to</td>
<td>Worldwide</td>
</tr>
<tr>
<td>Payment</td>
<td>FE Listing 100%</td>
</tr>
</tbody>
</table>

Germany - 2 days - USD +0.96 / item

Purchase price: USD 22.48

Qty: 1  Buy Now  Queue

0.0731 BTC
DrugsFromGermany (648) Level 5

Positive feedback (last 12 months): 98%

Detailed seller ratings:
- schnell bestellt und super
- Super
- fast for trust good product
- fast shipping in 2 days and good stealth
- SUPER

Total positive feedback: 348

Feedback:
- fast shipping in 2 days and good stealth
- 5x Hello Kitty 220mg MDMA Pink XTC-Pills

Buyer Statistics (since join date)
- Total disputes / orders: 0 / 0
- Total spendings: ---
- Feedback left: 0 (100.0% positive)
- Last online: Oct 28, 2015

Seller Feedback Ratings (last 12 months)

<table>
<thead>
<tr>
<th>1 month</th>
<th>6 months</th>
<th>12 months</th>
</tr>
</thead>
<tbody>
<tr>
<td>Positive</td>
<td>104</td>
<td>244</td>
</tr>
<tr>
<td>Neutral</td>
<td>1</td>
<td>5</td>
</tr>
<tr>
<td>Negative</td>
<td>0</td>
<td>4</td>
</tr>
</tbody>
</table>
[US FULLZ] - ALL STATES - SSN/DOB+ SUPERFRESH

Vendor: Skyscraper (280) (4.80★) (2)
Price: $0.0000977 ($1.04)
Ships to: Worldwide, Worldwide
Ships from: Internet
Escrow: No

41-75y.o USA Fullz with credit score 750+. Everyth

Vendor: valid_cc_info (1400) (4.92★) (a) 1008/5/15
Price: $0.00488 ($52)
Ships to: Worldwide, Worldwide
Ships from: Worldwide
Escrow: Yes

This listing is for FULLZ for persons who was born in 1940-1974. For younger FULLZ please visit my other listing: http://ichudifyeqm4idj.onion/viewProduct?offer=325189.223648

Buying this listing you will get:
Full name
Address
Phone
City
Zip
SSN
DOB
Credit score - For score from 750, just buy this listing for 40$. For 800+, specify in shipping method +10$.
Email: BM-2cVbNcn18dhfcefbaX73USLq4dYTtAxW7U@bitmessage.ch

Solutions to Common Problems! We are an organized criminal group, former soldiers and mercenaries from the FFL, highly-skilled, with military experience of more than five years. We can perform hits all around the world.

If you're asking yourself “Why someone would need to hire a killer online?”, we'll tell you, simply because it is anonymous. You can always find examples of contractors who collaborated with cops (when they were facing 20 years of prison), and you/the buyer could end up in the prison because of that. On the other hand, you can also find examples where police found who had the interest to put out a contract, and they can come to you and you can give your testimony (which would put the hitman in jail). So, it is of mutual interest to make everything anonymous. This website is hosted on a series of anonymous servers, with access to the Internet through the Tor network. You can access this site anonymously only through the Tor network, and we upload files to the server through the Tor network. You can make payments with an anonymous digital currency, either Bitcoins. It means we don’t know you and you don’t know us. We can’t send you to prison, and you can’t send us to prison. Of course you must take a risk when you pay in advance, but there is no interest. With risk comes reward. You take a risk, and someone can always cheat you. As we said, many criminals have the balls to do things to other people, but when they face 20 years of prison they begin to talk with the police. Risks about prison and money are always present. If you are not ready to take a risk, don’t contact this kind of organizations. And know, we are only one, real contractor there. Any other will try cheat you. — C'thulhu © 2010.
<table>
<thead>
<tr>
<th>Murder Types</th>
<th>Regular Person</th>
<th>Public Persons</th>
<th>1-2 Guards</th>
<th>3-5 Guards</th>
</tr>
</thead>
<tbody>
<tr>
<td>Regular</td>
<td>$45,000</td>
<td>$180,000</td>
<td>$360,000</td>
<td>$540,000</td>
</tr>
<tr>
<td>Missing in action</td>
<td>$60,000</td>
<td>$240,000</td>
<td>$480,000</td>
<td>$720,000</td>
</tr>
<tr>
<td>Death in accident</td>
<td>$75,000</td>
<td>$300,000</td>
<td>$600,000</td>
<td>$900,000</td>
</tr>
<tr>
<td>Cripple Types</td>
<td>Regular Person</td>
<td>Public Persons</td>
<td>1-2 Guards</td>
<td>3-5 Guards</td>
</tr>
<tr>
<td>Regular</td>
<td>$12,000</td>
<td>$48,000</td>
<td>$120,000</td>
<td>$180,000</td>
</tr>
<tr>
<td>Uglify</td>
<td>$18,000</td>
<td>$72,000</td>
<td>$160,000</td>
<td>$240,000</td>
</tr>
<tr>
<td>Two Hands</td>
<td>$24,000</td>
<td>$96,000</td>
<td>$200,000</td>
<td>$300,000</td>
</tr>
<tr>
<td>Family</td>
<td>$32,000</td>
<td>$32,000</td>
<td>$32,000</td>
<td>$32,000</td>
</tr>
<tr>
<td>Members</td>
<td>$48,000</td>
<td>$48,000</td>
<td>$48,000</td>
<td>$48,000</td>
</tr>
<tr>
<td>Simple</td>
<td>$3,000</td>
<td>$12,000</td>
<td>$30,000</td>
<td>$30,000</td>
</tr>
</tbody>
</table>
Black Death has moved. All existing customers have been provided with new address. This is the action we have to take in order not to become too popular.
You are being released as a huge generosity from Black Death Group. Your release does, however, come with a warning, and you should read the letter very carefully.

You are certainly aware of your value on human slavery market and must make a note that this isn't personal, this is business. For your release we have taken a number of factors into consideration.

A mistake was made by capturing you, especially considering you are a young mother that should have im no circumstances be lured into kidnapping. Second important factor you are very well aware of is your overall protection by one of our main and very well respected men who made a very clear and solid stance in your case.

You will, upon your landing in your home country cease any investigation activities related to your kidnapping. You also agreed to sneak a pre-determined set of information in to the media, and we will expect to see evidence that has been done in near future.

You and your family will, in no way ever talk about us in bad language and without respect. You have been treated fairly, with respect and we expect to hear exactly the same about us in return. You can release any information you have heard from MD while your holding as he would never give you any information that could harm our activities. We will not tolerate lying about anything that has happened.

You have also agreed to pay outstanding costs of your release of 50,000$. We expect that money to be paid in, in BitCoins within one month.

Any sort of disobedience with the above will result in your elimination.
How do criminals get caught?

- Attacks against Tor
- 0-day attacks
- Bad OpSec / Metadata leaks
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() by the
United States District Court for the Southern District of New York
altoid Jr. Member

I'm looking for the best person with experience in software architecture to join our company. The ideal candidate would have at least several years of web application development experience, with a strong understanding of software architecture as a must. Experience in a start-up environment is a plus, or at least someone who can adapt to a fast-paced, high-growth environment.

If interested, please send your answers to the following questions to rossulbricht at gmail dot com.

1) What are your qualifications for this position?
2) What interests you about bitcoin?
Protecting your networks

✧ Think about what is going out, not just coming in
  • NextGen Firewalls
  • Application control
  • SSL Decrypt
✧ Control what people can install
  • Don’t give admin permissions
  • Consider application whitelisting
✧ If you detect Tor activate Incident Response
  • Employee is doing something they shouldn’t, or…
  • Something/someone is in your network
Questions

셇 Stephen Heath, VP, Security
셇 Intrinium.com
셇 Email: stephen.heath@Intrinium.com
셇 Twitter: @hackerhiker