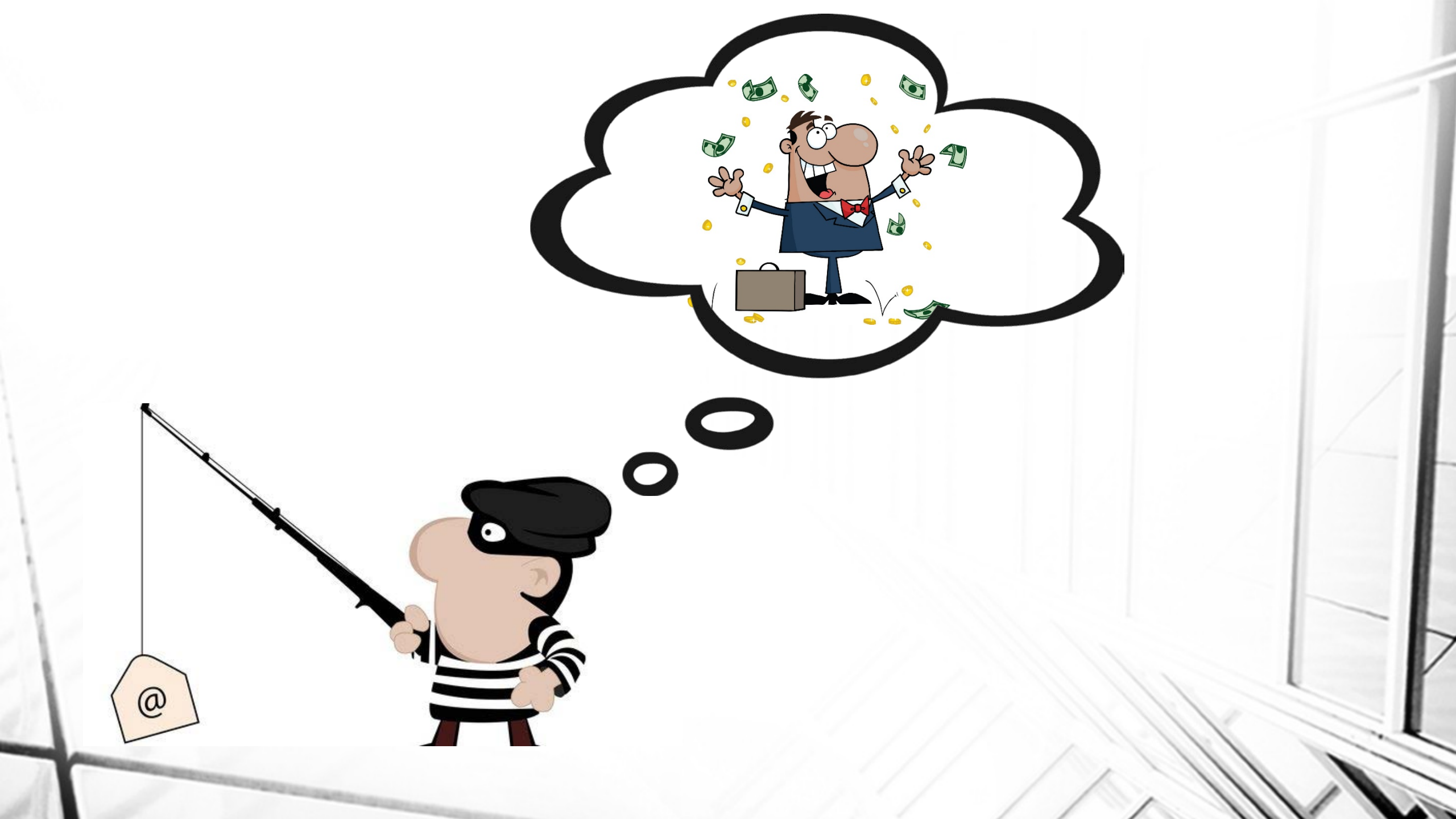
A Dive Into the Underground Markets

Alexis Michael, DInfoSec (cand.)
BSc, MSc, MBA, CISSP, CISA, CEH, EDRP, Security+




THE WEB
SURFACE WEB
DEEP WEB
Tor
DARK WEB

Darknet

- Darknet', colloquially, refers to a distinct network supporting cryptographically hidden sites
  - Appeared roughly in 2004
- While these tools are designed and intended to protect users from traffic analysis, which "threatens personal freedom and privacy, confidential business activities and relationships, they are also used by criminals operating online to protect their own freedom
- Darknets use unique software to allow use of the distributed network.
  - Most popular: • Tor • I2P • Freenet
- Tor architecture provides two services:
  - anonymous browsing (most popular - legitimate)
  - hosting of anonymous information exchanges (*.onion)

The anonymous Internet

Daily Tor users per 100,000 Internet users

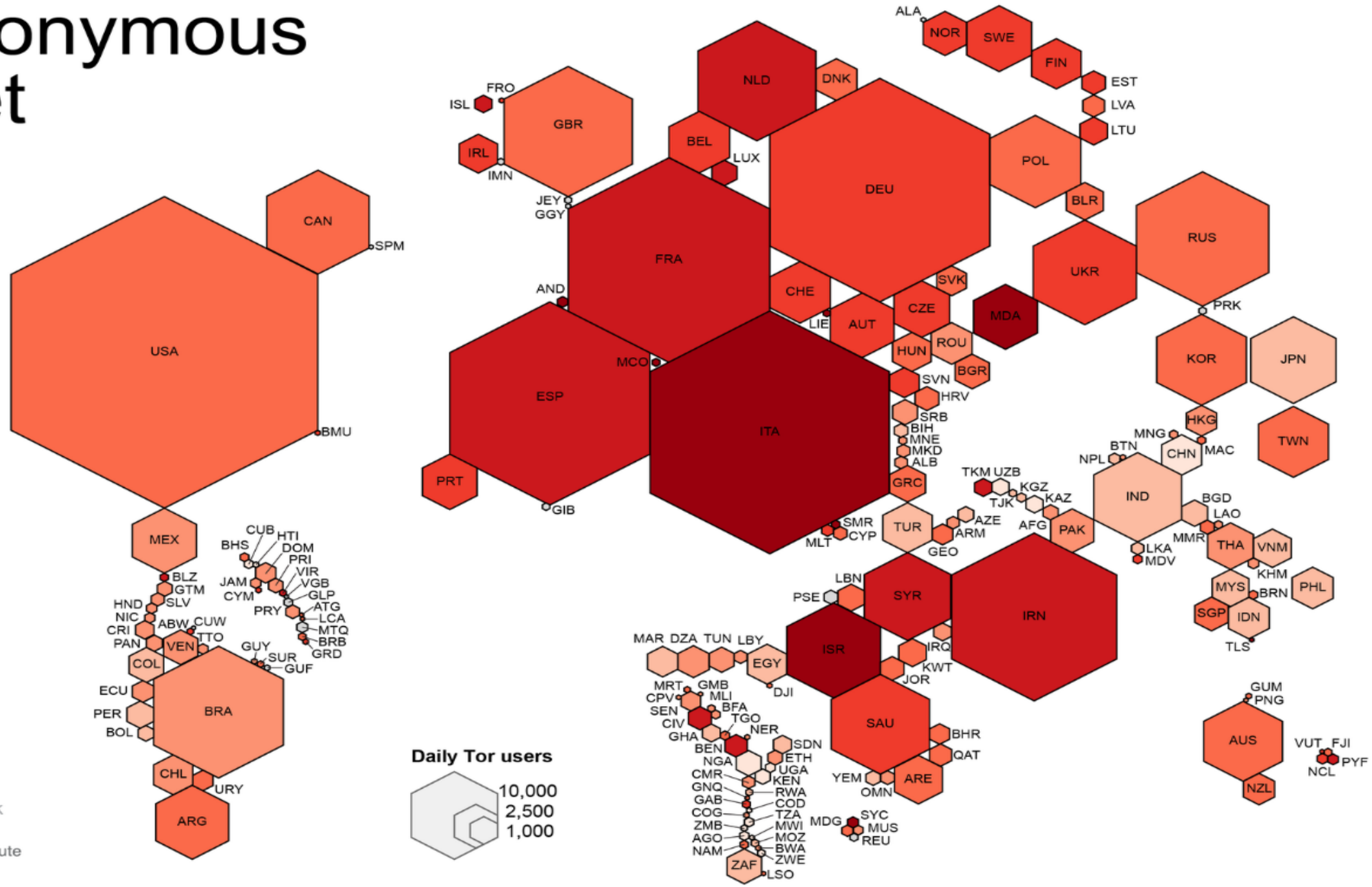
- > 200
- 100 - 200
- 50 - 100
- 25 - 50
- 10 - 25
- 5 - 10
- < 5
- no information

Average number of Tor users per day calculated between August 2012 and July 2013

data sources:
Tor Metrics Portal
metrics.torproject.org
World Bank
data.worldbank.org

by Mark Graham (@geoplace) and Stefano De Sabbata (@maps4thought)
Internet Geographies at the Oxford Internet Institute
2014 • geography.oii.ox.ac.uk

Oxford Internet Institute
University of Oxford



Underground Markets - Categories

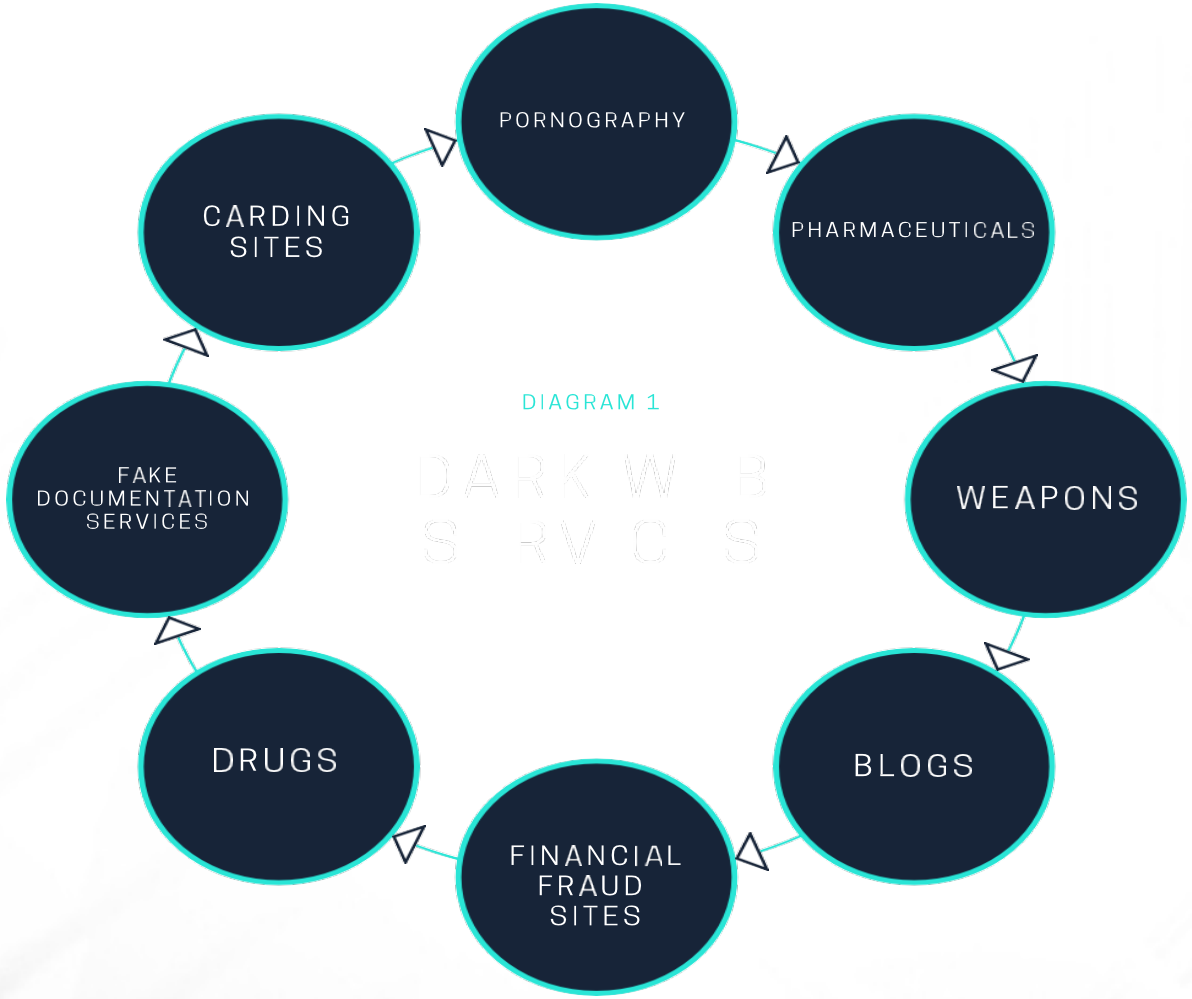


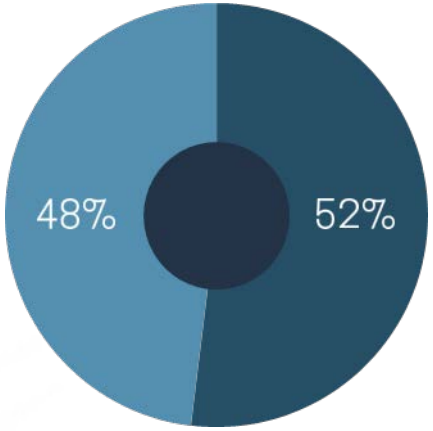
DIAGRAM 1

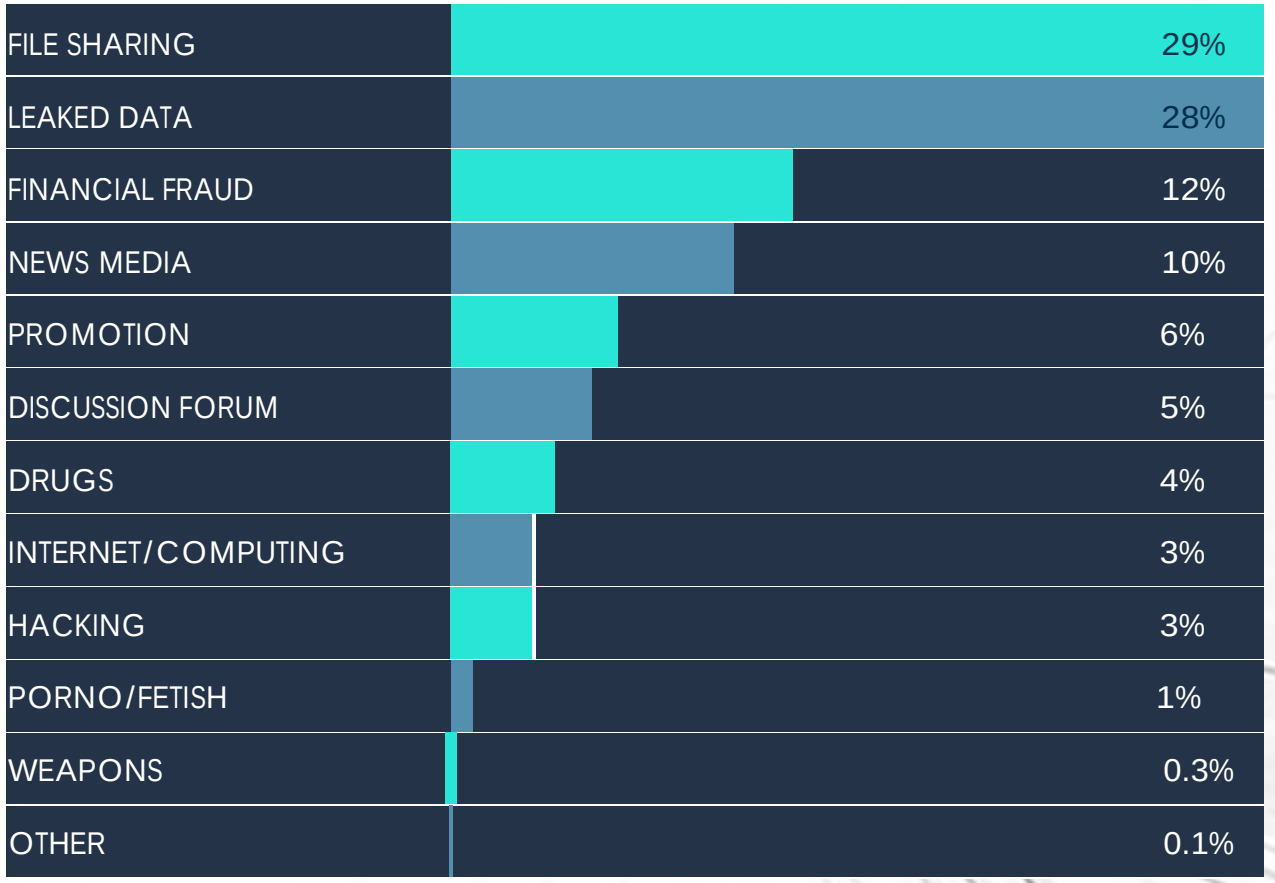
DARK WEB SERVICES

DeepLight Report, 2016

DeepLight Report 2016

Out of 29 500 sites examined





TorBrowser | Blue Sky Marketplace

blueskyplzv4fsti.onion/store/index

Blue Sky Store

Hi, t3ster! | Messages | Purchases | Support | BTC: 0 | Deposit BTC! | Logout

- **Cannabis** (400+)
  - Concentrate (50+)
  - Edibles (20+)
  - Hash (50+)
  - Seed (18)
  - Weed (300+)
- **Dissociatives** (20+)
- **Ecstasy** (100+)
  - MDMA (100+)
  - Methylone (50+)
- **Opioids** (50+)
- **Prescription** (200+)
  - Benzos (20+)
  - Opiates (20+)
  - Stimulants (9)
- **Psychedelic** (100+)
  - 2C (20+)
  - DMT (5)
  - LSD (50+)
  - Mushrooms (8)
  - Others (50+)
- **Stimulants** (100+)
  - Amphetamine (50+)
  - Cocaine (50+)
  - Meth (20+)

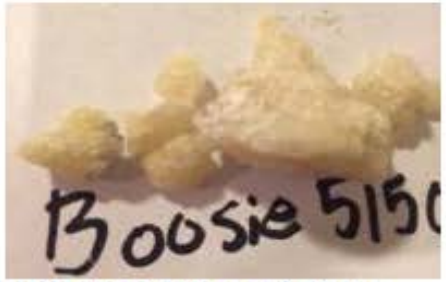
Sort by: By popularity Sort! 1 2 3 4 5 6 > Only show domestic products

7g Highgrade Dutch Super ...
$120 for 0.25oz ($480/oz) Weed
By MrCronk's Coff... (100+ ★)

1.1g Outdoor Strawberry K...
$16 for 0.04oz ($400/oz) Weed
By MrCronk's Coff... (100+ ★)

3.5g Of Cocaine **express...
$245 for 0.12oz ($2042/oz) Cocaine
By The NCZ Store (100+ ★)

1.1g Highgrade Dutch Supe...
$25 for 0.04oz ($625/oz) Weed
By MrCronk's Coff... (100+ ★)



| 1 Gram Hq Mdma| 1 Gram ...
$50 for 0.04oz ($1250/oz) MDMA
By NW Connection (100+ ★)

1$ Trips The Dollar Store...
$1.25 for 1 ($1.25/each) 2C
By Cloud9 (84 ★)

Super Sour Diesel - Sativ...
$36 for 0.12oz ($300/oz) Weed
By Deliverator (100+ ★)

3.5 Grams Of Pure Uncut ...
$270 for 1 ($270/each) Cocaine
By tocoolforschool14 (100+ ★)

armory34omvkkmgr.onion/index.php?route=common/home

Startpage

ARMORY

Currency
฿ Ł $

Shopping Cart
0 item(s) - $0.00

Search

Welcome visitor you can login or create an account.

Home | Wish List (0) | My Account | Shopping Cart | Checkout

Package Deals | Pistols | Rifles | Shotguns | NFA Weapons | Accessories | Armor | Ammunition | Military

Specials

AKM Gen2
~~$3,605.98~~ $2,800.00
Add to Cart

CIA Model PAP
~~$1,956.64~~ $1,401.56
Add to Cart

CZ-USA P07 DUTY
~~$920.82~~ $820.00
Add to Cart

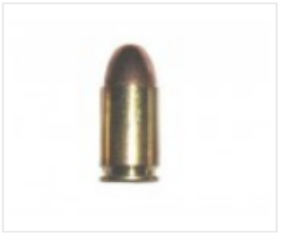
This is a site catalog, please email us with your order. All items sold under your choice of .onion escrow.

Bestsellers

Walther P22
$752.65
Add to Cart

Glock 17 & Gemtech Tundra
~~$2,223.45~~ $1,599.99
Add to Cart

Beretta PX4 Storm Type F
$1,223.90
Add to Cart



9x19mm Parabellum
$0.30
Add to Cart

Glock 26 Gen4
$1,027.94
Add to Cart

Glock 17 Gen4
$1,027.94
Add to Cart

CIA Model PAP
~~$1,956.64~~ $1,401.56
Add to Cart

Glock 32 Gen4
$1,027.94
Add to Cart

Categories

- Package Deals (4)
- Pistols (87)
- Rifles (66)
- Shotguns (4)
- NFA Weapons (84)
- Accessories (68)
- Armor (28)
- Ammunition (33)
- Military (44)

Shipping Points

- Australia (NewCastle) - $290
- Australia (Perth) - $340
- Austria (Graz) - $270
- Canada (Toronto) - $190
- Canada (Vancouver) - $190
- France (Le Mans) - $270
- Germany (Dresden) - $220
- Ireland (Tuam) - $290
- Italy (Modena) - $280
- N. Ireland (Belfast) - $340
- Netherlands (Breda) - $320
- Norway (Drammen) - $240
- Russia (Vyborg) - $190
- Finland (Tornio) - $290

Dell SecureWorks – UG Markets Report (2016)

Price List for Hacker Goods and Services

Credit Cards

	Price in 2013	Price in 2014	Recent Prices
Visa and MasterCard (U.S.)	$4	$4	$7
Visa Classic and MasterCard (U.S.) with Track 1 and Track 2 Data	$12	$12	$15
Visa Classic and MasterCard (Canada, Australia, and New Zealand) with Track 1 and Track 2 Data	$19 – $20	$19 – $20	$25
Visa Classic and MasterCard Standard (EJ) with Track 1 and 2 Data	$28	$28	$40
Visa Classic and MasterCard Standard (U.K) with Track 1 and Track 2 Data	$19 – $20	$19 – $20	$40
Visa Classic and MasterCard Standard (Japan and Asia) with Track 1 and Track 2 Data	$28	$28	$50

Hacking Email and Social Media Accounts

	Recent Prices
Popular U.S. Email Accounts (Gmail, Hotmail, Yahoo)	$129
Popular Russian Email Accounts (Mail.ru, Yandex.ru, and Rambler.ru)	$65 – $103
Popular Ukranian Email Accounts (Ukr.net)	$129
Popular U.S. Social Media Accounts	$129
Popular Russian Social Media Accounts (VK.ru and Ok.ru)	$194
Corporate Email Accounts	$500 per mailbox
IP address of Computer User	$90

Table 1: Rates for hacking social media and email accounts

Mail.ru	5,000 rubles (approximately $65)
Yandex.ru	7,000 rubles (approximately $90)
Rambler. Ru	8.000 rubles (approximately $103)
Ukr.net	10,000 rubles (approximately $129)
Gmail.com, Yahoo.com, Hotmail.com	10,000 rubles (approximately $129)
Facebook.com	10,000 rubles (approximately $129). Please note: the victim's password stays the same.
IP address of computer user	7,000 rubles (approximately $90)
Corporate email account	$500 per mailbox
VKontakte (VK) social media account	15,000 rubles (approximately $194)
Odnoklassniki (OK.ru) social media account	15,000 rubles (approximately $194)

Tools

	Price in 2013	Price in 2014	Recent Prices
Remote Access Trojans (RATs)	$50 – $250	$20 – $50	$5 – $10
Crypters	N/A	$50 – $150	$80 – $440
Angler Exploit Kit			$100 – $135

Identities, Passports, Social Security Cards and Other Documents

	Price in 2013	Price in 2014	Recent Prices
US Fullz	$25	$30	$15 – $65
Fullz (Canada, U.K.)	$30 – $40	$35 – $45	$20 (Canada) $25 (U.K.)
U.K. Passport Scan			$25
Physical Counterfeit Passports (non-U.S.)	N/A	$200 – $500	$1,200 to $3,000 (European)
Physical Counterfeit Passports (U.S.)			$3,000 to $10,000
Templates for U.S. Passports			$100 – $300
New Identity Package, including scans of Social Security Card, Driver's License and, matching utility bill		$250; matching utility bill an additional $100	$90

A hacker seen advertising Distributed Denial of Service (DDoS) attacks states in his ad that he is: "Always online 24/7."

Now that is customer service.

Hacking Services

	Price in 2013	Price in 2014	Recent Prices
Hacking Tutorials	N/A	$1 each to $30 for 10 (depending on the tutorial)	$20 to $40 for multiple tutorials
Hacking Website (stealing data)	$100 – $300	$100 – $200	$350
DDoS Attacks	Per Hour: $3 – $5 Per Day: $90 – $100 Per Week: $400 – $600	Per Hour: $3 – $5 Per Day: $60 – $90 Per Week: $350 – $600	Per hour: $5 – $10 Per Day: $30-$55 Per Week: $200 – $555

DDoS Attacks; Free 5-10 Minute DDoS Tests Offered

One of the most interesting items we found for sale on the Russian Underground were full business dossiers on companies located within the Russian Federation. The hackers are selling information and documents from Russian organizations, including all of the credentials associated with a company's various bank accounts (account numbers, logins, passwords, tokens). They are also providing the company's original articles of incorporation, lease agreements, and the company's Tax Identification Number (TIN), also known as an Employer Identification Number. TIN is a number used to identify entities for tax-related purposes such as filing tax returns, or other actions such as opening a bank account.

₽ The price for the Russian company dossiers ranges between 40,000($547) and 60,000 rubles ($822).

According to one hacker/seller of such data, buyers get two full days to review the company documents, and the seller is also willing to work through a "Guarantor Service."

How can I protect my organization?

- **YOU ARE A TARGET -** Take all necessary measures to protect your organizational environment
- **Measures are not only of technical nature –** Security is everyone's responsibility
- **Create a security culture within your organization -** Overall organizational security is only as strong as the weakest link
- **IT is NOT Information Security and security is NOT just IT**
- **Make sure your Information Security team monitors these underground markets**