



DAY 2


Instructors:

Joseph Mlodzianowski

Omar Santos

DISCLAIMER/ WARNING

- The information provided on this training is **for educational purposes only**. The authors, O'Reilly, or any other entity is **in no way responsible for any misuse of the information**.
- Some of the tools and technologies that you will learn in this training class may be illegal depending on where you reside. Please check with your local laws.
- Please practice and use all the tools that are shown in this training in a lab that is not connected to the Internet or any other network.



Do not hack your neighbor

What we
covered
yesterday...

- **Introduction to Passive Recon and OSINT**
- **Using Recon-NG and SpiderFoot**
- **Using Shodan and the Shodan API**
- **Using Maltego and the Harvester**
- **Introduction to Active Recon**
- **Port and Vulnerability Scanning**
- **Subdomain Enumeration**
- **Directory Enumeration**
- **Account Enumeration**

Day 2 - Agenda

- **The Deep Web vs. the Dark Web**
- **Introduction & Technical Tor**
- **Using the Tor Browser**
- **Using Proxies and Proxy Chains**
- **Creating Remote worker, commercial and your own VPN Server's in the Cloud**
- **Staying Safe when Performing Dark Web Research, Persona's**
- **Tools and Tips on Performing Dark Web Reconnaissance**



Pre-requisites

- You must be familiar with virtualization technology (i.e., Virtual Box, VMWare, etc.)
- You must be familiar with basic Linux commands, basic networking, and basic cybersecurity concepts.

Other Classes

- Dark Web Rep and Recon for the CISO
- Ultimate Linux Hardening Bootcamp
- Ethical Hacking Recon on the Surface and Dark Web
- Bug Bounty Hands-on Workshop
- Building Secure VPN's (SVPN) for the Enterprises

<https://www.oreilly.com/live-events/darknets-and-the-dark-web-recon-for-the-ciso/0636920074169/0636920078242/>



The Webs of the Internet

- **The Surface Web**
 - **The Deep Web**
 - **The Dark Web**
 - **& Darknet's**





Bing
Youtube
Google
Yahoo
E-Commerce



Instagram
Facebook
Twitter
Blogs

academic papers

Deep Web

legal and medical documents

Unindexed websites

90%

hackers

Private forums

Scientific reports

Stolen credit cards

Dark Web

encrypted forums

legal and illegal information

6%

Threat actors

illegal trade

bad actors

drugs

Weapons





Internet

World Wide Web
The internet as accessible through a browser

Internet

Surface Web
Portions of www that are indexed by search engines.

DeepWeb

portions of the web accessible through a browser but not indexed by search engines or requires special API access

all services, routed and all protocols

Dark Web
TOR

12P
FreeNet
ZeroNet
GUNnet

Web / Dark Intersection

Dark net
DarkNet services
chat, file sharing, email,
requires special client,
agent, VPN for access

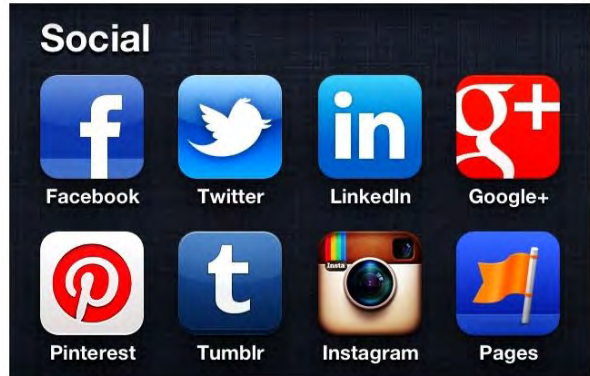


Surface, Deep & Dark Web

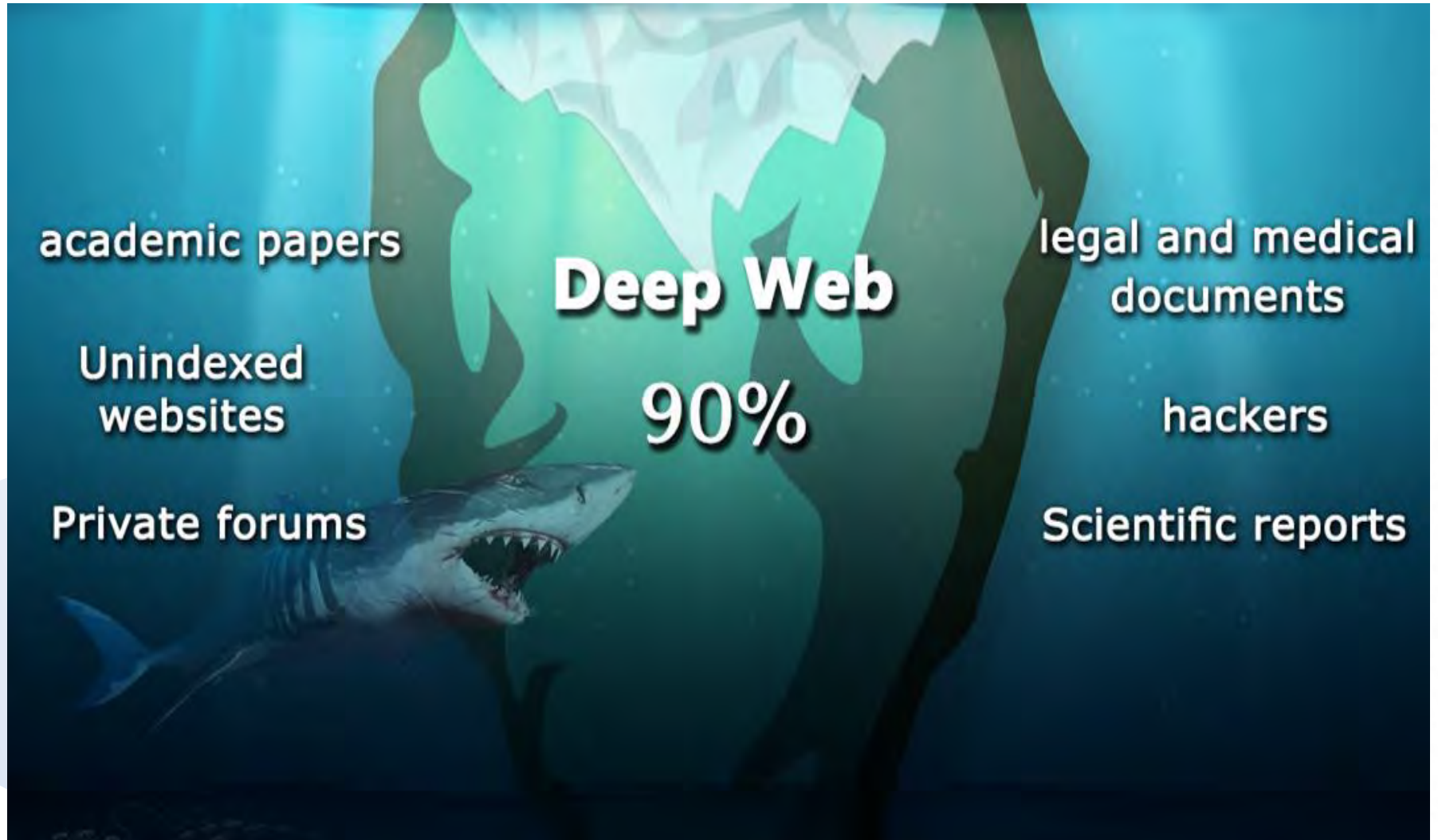
The Content on the surface web (ClearNet) Clearweb, it is estimated that only 6% of it is indexed and searchable via search engines.

Surface Web

- Facebook
- Reddit
- Myspace
- Google
- Yandex
- Wikipedia
- Yahoo
- Twitter
- Bing



The uncatalogued Internet





Search engines are how humans access the surface web.

When search engines like google, Bing or Yahoo are unable to properly connect to a site, it's not added.

Search engines do what's called Crawling, they Crawl a web page following all links like a spyder web, however a dynamic page like one that get generated when you ask a online database a question, since the crawler can not follow links deeper past the search box, it is unaware of the rest of the site and its content, because it can not index it, these sites get left out.

The vast majority of the Deep Web holds pages with valuable information. Estimates are that 68% of websites are databases and backend systems. Among the world's largest are the U.S. National Oceanic and Atmospheric Administration, JPL, NASA, and others -- all of which are public. The next batch has pages kept private by companies that charge a fee to access them, like Research, legal documents, government documents on LexisNexis and Westlaw, Stockmarket and Trading systems as well as academic journals, and another 13% are pages that require/host direct access (user/pwd) to gain access to, message boards, personnel files, academic papers and journals, forums and more.





The Deep Web - Search engine Context

The content of the deep web can be located and accessed by a direct URL or IP address, but may require a password, a vpn or other security access control mechanisms, like certificates, MFA, etc. There are many methods that prevent web pages from being indexed by traditional search engines, one or more of the following:

Contextual web: Pages with content varying for different access contexts (ranges of client IP addresses or previous navigation sequence).

Dynamic content: Dynamic pages, which are returned in response to a submitted query or accessed only through a form, especially if open-domain input elements (such as text fields) are used; such fields are hard to navigate without domain knowledge.

Limited access content: sites that limit access to their pages in a technical way, such as using the Robots Exclusion Standard or CAPTCHAs, or no-store directive, which prohibit search engines from browsing them and creating cached copies.

Non-HTML/text content: textual content encoded in multimedia (image or video) files or specific file formats not handled by search engines.

Private web: Sites that require registration and login (password-protected resources).

Scripted content: pages that are only accessible through links produced by JavaScript as well as content dynamically downloaded from Web servers via Flash or Ajax solutions.

Software: certain content is intentionally hidden from the regular Internet, accessible only with special software, such as vpn, Tor, I2P, or other deep and darknet software.

Robots.txt files: A list of directories a crawler can and can not (or should not) crawl.

Most websites have a clear crawling policy which states what directories crawlers can or cannot traverse. Check-out robots.txt, usually placed in the root of the website. <https://www.cnn.com/robots.txt>

```
Sitemap: https://www.cnn.com/sitemaps/cnn/index.xml
Sitemap: https://www.cnn.com/sitemaps/cnn/news.xml
Sitemap: https://www.cnn.com/sitemaps/sitemap-section.xml
Sitemap: https://www.cnn.com/sitemaps/sitemap-interactive.xml
Sitemap: https://www.cnn.com/ampstories/sitemap.xml
Sitemap: https://edition.cnn.com/sitemaps/news.xml
Sitemap: https://www.cnn.com/sitemap/article/cnn-underscored.xml
Sitemap: https://www.cnn.com/sitemap/section/cnn-underscored.xml
User-agent: *
Allow: /partners/ipad/live-video.json
Disallow: /*.jsx$
Disallow: *.jsx$
Disallow: /*.jsx/
Disallow: *.jsx?
Disallow: /ads/
Disallow: /aol/
Disallow: /beta/
Disallow: /browsers/
Disallow: /cl/
Disallow: /cnews/
Disallow: /cnn_adspaces
Disallow: /cnnbeta/
Disallow: /cnnintl_adspaces
Disallow: /development
Disallow: /editionssi
Disallow: /help/cnnx.html
Disallow: /NewsPass
```

Another way of providing a crawling policy is through meta tags included in the HTML of individual pages. There is a special meta tag called robots, which can be used with combinations of values of two aspects: **index** or **noindex** (ie: allow or disallow this page to be crawled) and follow or nofollow.

```
<meta name="robots" content="index,nofollow">
<Disallow: /*.jsx$>
```

This statement says the page can be crawled, but links on the page can not be followed.

The appropriate method is to control directories/files/folders access via “rights” restrictions, to ensure systems and people can’t access sensitive data.

If you’re a hacker and you see this list, what’s the first thing that comes to mind ?

The Deep Web



Shodan The Search Engine for Hackers

html:"tor" html:"market"

PublicWWW Log In

Search bar with input field containing "tor market" and a search button.

Too many results? Try a phrase search with quotes: "Tor market". Need more results? Try internal pages search.

query syntax 35404 web pages in 0.30 s. [URLs] [CSV] [CSV+snippets]

| Rank | Url | Snippets |
|--------|---|---|
| 54 | https://mail.ru/ | ntrol: no-cache,no-store,must-revalidate Pr-460px).icon_social_market{background-position |
| 14 078 | https://www.swtor.com/ | tion: https://www.swtor.com/ Content-Type: row"> Cartel Market Additions: Game Upd |
| 18 008 | https://www.bestchange.com/ | Cache-Control: no-store, no-cache, must-re e-currency exchange market, and reflect them i |
| 4 839 | https://www.spotracc.com/ | Cache-Control: no-store, no-cache, must-re www.spotracc.com/nfl/market-value">» Mar |

Try * or port:3306 or protocol:mysql or asn:16509 or ip:"13.0.0.0/8"?

Leaks Enter search query Search

Search Hosts html:"tor" Search

Services: 2.1B IPv4 Hosts: 215.3M IPv6 Hosts: 21.8M Virtual Hosts: 559.1M

VIEW DOCUMENTATION LEARN MORE ABOUT CENSYS

INTERNET ARCHIVE

WayBack Machine

looksmart

metacrawler

ZoomEye——网络空间挂图作战，资产情报唾手可得
面向全球用户 永久免费

<https://www.searchenginewatch.com/>

88.99.210.194

static.194.210.99.88.clients.your-ser...

443/PSA/http/TCP IDC

Germany, Falkenstein

2022-05-27 02:47

Hetzner Online GmbH

hetzner.com

ASN: AS24940

TITLE: 302 Found

Кафель (плитка) и сантехни...

Banner File

HTTP/1.1 302 Moved Temporarily

Server: nginx

Date: Thu, 26 May 2022 18:47:45 GMT

Content-Type: text/html

Content-Length: 138

Connection: close

Location: https://_/

X-Content-Type-Options: nosniff

X-Frame-Options: SAMEORIGIN

<html>

<head><title>302 Found</title></head>

<body>

<center><h1>302 Found</h1></center>



Deep Web Starting points

Here are a few more ways to search for content on the Deep Web:

- [BizNar](#)
- [Data.gov](#)
- [Google News](#)
- [Google Scholar](#)
- [govinfo](#)
- [GreyNet International](#)
- [OpenGrey](#)
- [SSRN](#)
- [TechXtra](#)
- [UW Libraries Articles & Research Databases](#)
- [Washington Open Data](#) (check your state)
- [WorldCat](#)
- [WorldWideScience](#)
- [Instant Checkmate](#)
- [TruthFinder](#)





Deep Web Site Comparison

Make the mental shift from *find the content* to *find a doorway to the content*.

Look for databases - searchable databases of information, research, or data about a specific topic.

- Try searching for a subject term and the word database.
 - Family Connections
 - Credit Card database
 - Public records database
 - Crime database
 - Languages database
 - Family Genealogy
 - Toxic chemicals database
 - Schools, Highschool, Collage
 - Local Government Property Databases
 - County Marriage License Databases

Deep web academic search comparison

| | Full-text? | Hosts Content? | Free Service? | Paywall? | Downloadable content? | Copy/Paste? | In-document search? | Updated regularly? |
|---------------------------------------|------------|----------------|---------------|----------|-----------------------|-------------|---------------------|--------------------|
| Google Scholar | ✓ | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| ISTOR | ✓ | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Archive.org | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Library of Congress | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Osti.gov | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Science.gov | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| The National Archives | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| HighWire Press | ✓ | ✓ | | ✓ | | | | ✓ |
| Encyclopedia Britannica | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| FRED | ✓ | ✓ | ✓ | | ✓ | ✓ | ✓ | ✓ |
| Google Books | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Scribd | ✓ | ✓ | ✓ | ✓ | ✓ | | ✓ | ✓ |
| Project Gutenberg | ✓ | ✓ | ✓ | | ✓ | ✓ | | ✓ |
| The Online Books Page | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | ✓ |
| Getty Research Institute | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | ✓ |
| Law Library of Congress | ✓ | ✓ | ✓ | | ✓ | ✓ | ✓ | ✓ |
| THOMAS (Library of Congress) | ✓ | ✓ | ✓ | | ✓ | ✓ | ✓ | ✓ |
| LexisNexis | ✓ | ✓ | | ✓ | ✓ | ✓ | | ✓ |
| PubMed | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Globalhealthfacts.org | ✓ | ✓ | ✓ | | ✓ | ✓ | ✓ | ✓ |
| New England Journal of Medicine | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| US Geologic Survey | ✓ | ✓ | ✓ | | ✓ | ✓ | ✓ | ✓ |
| US National Map by USGS | ✓ | ✓ | ✓ | | ✓ | ✓ | ✓ | ✓ |
| USGS Real-Time Water Data | ✓ | ✓ | ✓ | | ✓ | ✓ | ✓ | ✓ |
| USGS Earthquake Hazards Program | ✓ | ✓ | ✓ | | ✓ | ✓ | ✓ | ✓ |
| The SAO/NASA Astrophysics Data System | ✓ | ✓ | ✓ | | ✓ | ✓ | | ✓ |
| Academic Index | ✓ | | ✓ | | ✓ | ✓ | ✓ | ✓ |
| IEEE Xplore Digital Library | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| TechXtra | ✓ | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| ScienceResearch.com | ✓ | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Arxiv | ✓ | ✓ | ✓ | | ✓ | ✓ | ✓ | ✓ |
| DeepDyve | ✓ | ✓ | | ✓ | ✓ | ✓ | ✓ | ✓ |
| VideoLectures.net | | ✓ | ✓ | | ✓ | | | ✓ |



The Deep Web Search

<https://archive.org/web/> | The Way-Back Machine 538 Billion web pages saved over time

<https://researchworks.oclc.org/archivegrid/> Archive Grid | 5 Million Records of Archival material family history

<https://www.base-search.net/> Base | Over 120 Million Records and 6000 resources from Bielefeld University in Germany

<https://foiaproject.org/data-tools/> FOIA Project | Search the Freedom of information database with millions of records

<https://doaj.org/> The Directory of Open Access Journals is a deep internet search engine that provides access to academic papers.

<https://elephind.com/>: Historical Newspaper Archives

<http://vos.ucsb.edu/> : Voice of the Shuttle went live in 1994, boasts one of the most impressive collections

<https://yippy.com/> : used to be Clusty, a meta search engine that combines the results of several search engines

<http://www.directsearch.net/> : list of hundreds of specialty databases and search engines

<https://oedb.org/ilibrarian/research-beyond-google/> : Since 2006, Comprehensive free courses and materials.

https://www.nts.gov/_layouts/ntsb.aviation/index.aspx : NTSB Aviation Accident Database

<https://library.fvtc.edu/Tools/DeepWeb> : Fox Valley Technical

<https://lookahead.surfswax.com/> : Currently locked

<https://startpage.com> | Search engine, non tracking similar to duckduckgo

<http://vlib.org> | www Virtual Library

<http://www.artsages.com/VLbrowsing/index.php> | Virtual Library advanced

Baidu | Yandex | Qwant |



15 min.



Exercise 1

LAB 1

The Dark Web



Warning



Stolen credit cards

legal and illegal
information

illegal trade
drugs

Dark Web

4%

encrypted forums

Threat actors

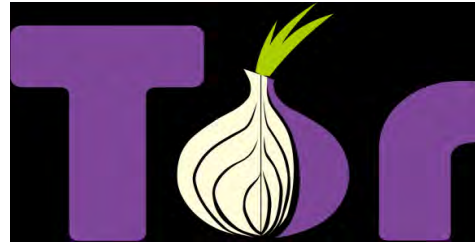
bad actors

Weapons



TOR

NOTICE: If you have not installed Tor **please wait** until we can provide you with the appropriate configuration, process and that you understand the risks.



We provide you with the Process, Procedures on how to build a hardened system and then best practices to make your activities are secure and more anonymous.





The Dark Web

Dark Web refers to specific networks that support cryptographical protected and hidden sites. Where digital privacy and the gradual development of secure networks as alternatives to internet sites that couldn't be easily censored has seen an explosion.

Piracy as well as illegal activity thrive in the dark, as hidden hosts are harder to locate and sue or even attribute to a person. Modern darknets use unique software to allow use of the distributed network. The most notable examples today are Tor, I2P and Freenet. The fluid architecture of these networks makes estimating their size difficult, from the last few researcher reports it appears that Tor is the largest.

Tor - The Onion Router:

Hundreds of Dark Web sites pop up and turned-down everyday

The Tor web addressing is a 56bit, numbers and letters that can seem obfuscated



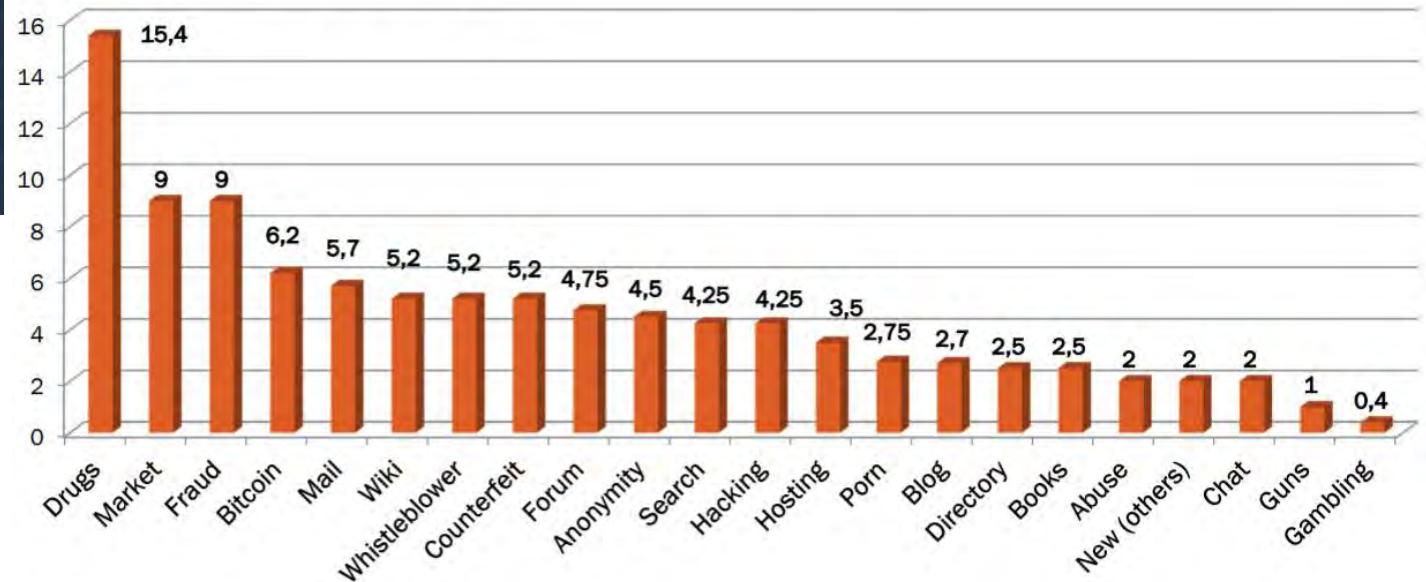


The Dark Web - Breakdown of Traffic

| | |
|--------------------|------|
| FILE SHARING | 29% |
| LEAKED DATA | 28% |
| FINANCIAL FRAUD | 12% |
| NEWS MEDIA | 10% |
| PROMOTION | 6% |
| DISCUSSION FORUM | 5% |
| DRUGS | 4% |
| INTERNET/COMPUTING | 3% |
| HACKING | 3% |
| PORNO/FETISH | 1% |
| WEAPONS | 0.3% |
| OTHER | 0.1% |

State of the Art Hidden Services in Tor

- authors analyzed more than 80.000 hidden services, finding:
 - 85% of HS are up for less than 5 days,
 - +100 new HS come online,
- There is increased usage by malware (botnets, ransomware, etc.) in relation to the surface web.



The Darkweb – Seized Sites



THIS HIDDEN SITE HAS BEEN SEIZED
and controlled since June 20

by the Dutch National Police in conjunction with the Bundeskriminalamt, Lietuvos Policija, Federal Bureau of Investigation and Europol, under the authority of the Dutch National Prosecutor's Office and the Attorney General's office of the Federal State of Hesse (Germany).



The Dutch National Police have located Hansa Market and taken over control of this marketplace since June 20, 2017. We have modified the source which allowed us to capture passwords, PGP-encrypted order information, IP-addresses, Bitcoins and other relevant information that may help enforcement agencies worldwide to identify users of this marketplace. For more information about this operation, please consult our hidden server profile: [profile.politie.nl/2seu.0h100](#).

This seizure was part of **Operation Bayonet**, which includes the takeover of Hansa Market by the National Police of the Netherlands and the takeover of AlphaBay Market by the Federal Bureau of Investigation of the United States of America on July 4, 2017.

 HANSA  AlphaBay Market

OPENBAAR MINISTERIE  POLITIE  EUROPOL



THIS WEBSITE HAS BEEN SEIZED

This domain has been seized by the Federal Bureau of Investigation pursuant to a seizure warrant issued by the United States District Court for the Central District of California under the authority of 18 U.S.C. §1030(i)(1)(A) as part of coordinated law enforcement action taken against illegal DDoS-for-hire services.

This action has been taken in coordination with the United States Attorney's Office of the District of Alaska, the Department of Justice Computer Crime and Intellectual Property Section, and



The Dark Web and Darknets



<https://www.torproject.org>

Anonymous Internet Proxy Network
Data is Routed through relays
Regular internet and darkweb privacy



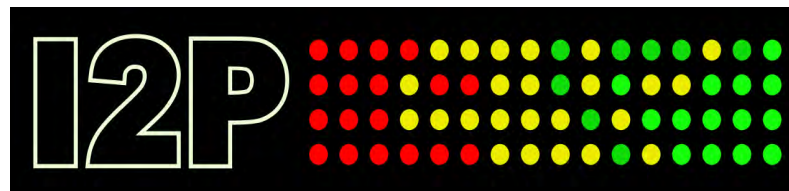
<https://freenetproject.org>

Anonymous data publishing network
Users Share portions of their bandwidth
independent networks can be shared



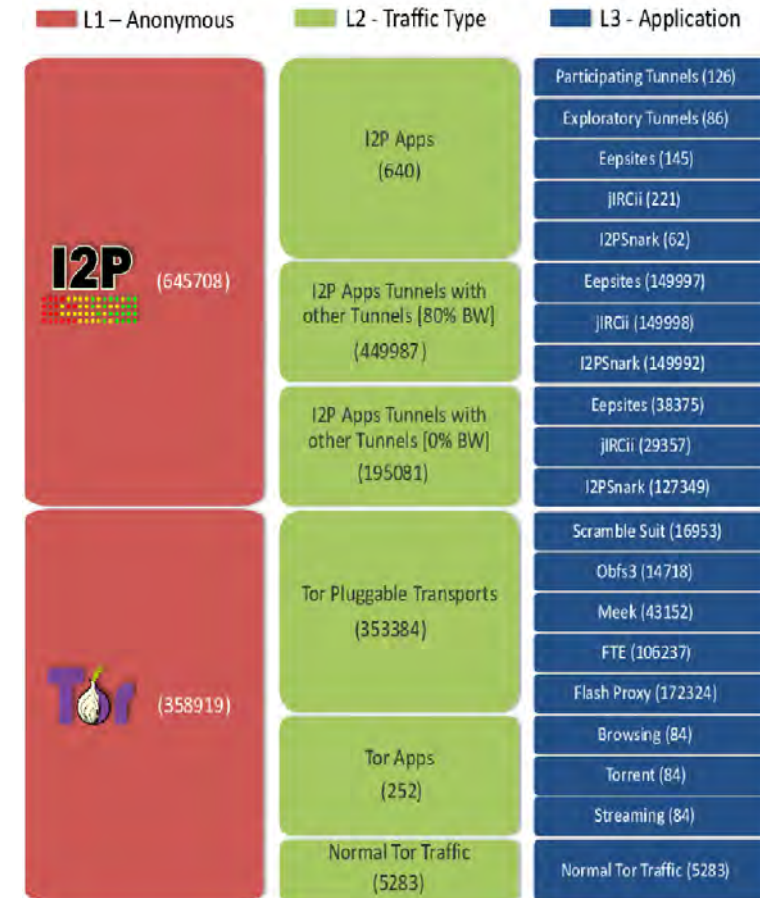
<https://zeronet.io>

Anonymous network using Tor
uncensorable websites using Bitcoin
Cryptography using BitTorrent Network



<https://geti2p.net>

Anonymous peer-to-peer Network
Garlic Routing with Unidirectional Tunnels
Super Slow and buggy





Dark Web & Dark Net Mobile



Group: Carders [Getbette.biz] – [Dumps][Cc][Cvw]
[Dumps+Pin][Track2 / Track1+Track2]

Group: Narcotic Express DE ❄️ 🚗

Group: Whatsapp Hacking Telegram

Group: Free Premium Accounts – Netflix•accounts•free•
premium•hotstar•disney•plus•amazon•prime•hulu•voot•
spotify•altbalaji•hack.

Telegram: telegram-group.com

Discord: top.gg & disboard.org

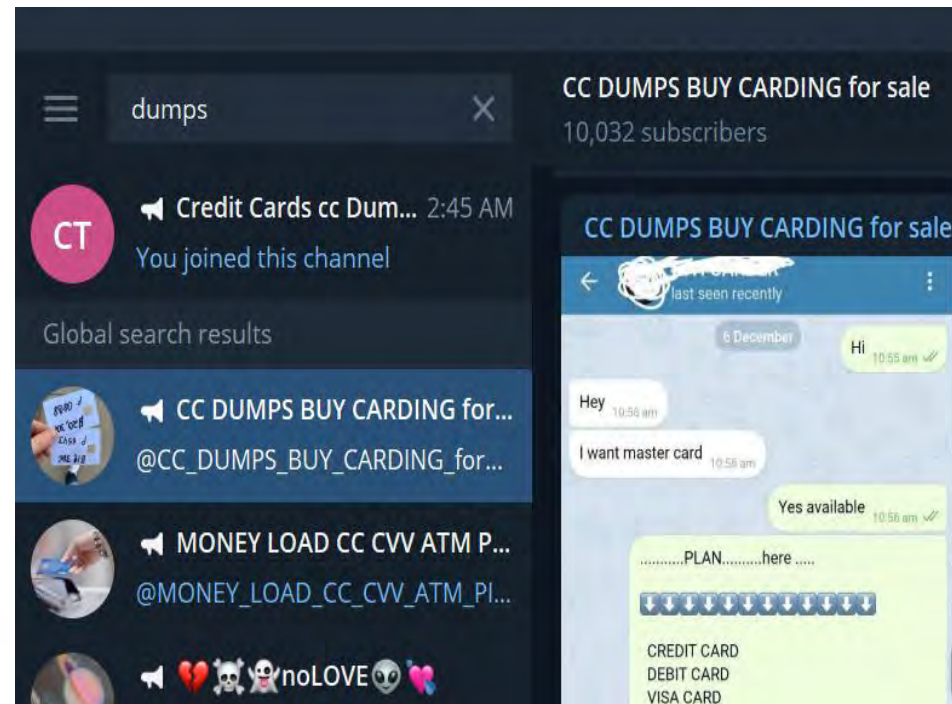
```

youtube.com/theunknon

[+] Choose a group to scrape members :
[0] - MaxBounty Killers
[1] - ANONYMOUS HACKERS CHAT
[2] - Blogging QnA Soldiers- Help each other
[3] - TERMUX CYBER [COMMUNITY]™
[4] - InFoTel Group
[5] - Blogging Pro Tips
[6] - True Blogging
[7] - Team Blogger - Discussion
[8] - SeoBlogGuide Discussion
[9] - Affiliate Marketing
[10] - Cyber Security Community Kerala
[11] - Amazon web services
[12] - AndroidHackerX Support
[13] - EvilChat
[14] - Cyber Hackers United [community]™
[15] - Telegram Bots Community
[16] - HACKING MANIAC
[17] - DummiesHub Group
[18] - Digital Seller Market |N | DSM |
[19] - Global Carders
[20] - Official DedSec Group
[21] - AndroNix
[22] - Tech expert 🔥🔥🔥 |BLOGGING⚡ |YOUTUBING🌟🌟 |DIGITAL MARKETING🌟🌟🌟🔥🔥🔥
[23] - Cybersecurity & Forensics
[24] - Affiliate Marketing | Eng
[25] - FTU CHAT [FTU]
[26] - Ask Akshay Hallur
[27] - IT Solutions Hub

[+] Enter a Number : 26
[+] Fetching Members...
[+] Saving In file...
[+] Members scraped successfully.
$

```



Dark Web.sh – dedicated to Darknet Research

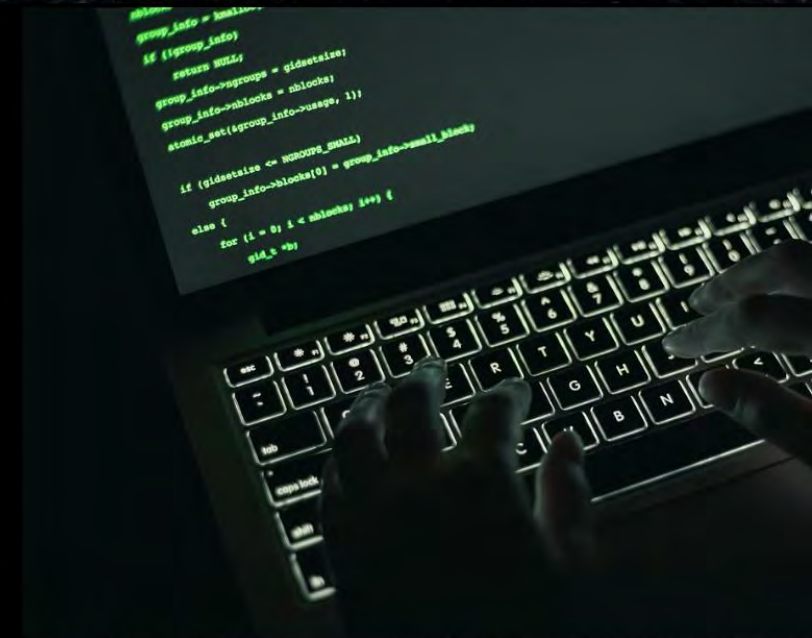
Dark Web ● SH

Training: Reputation, Research and Investigations



Class Curriculum

<https://darkweb.sh/discord>



Class Platform

Introduction to Tor

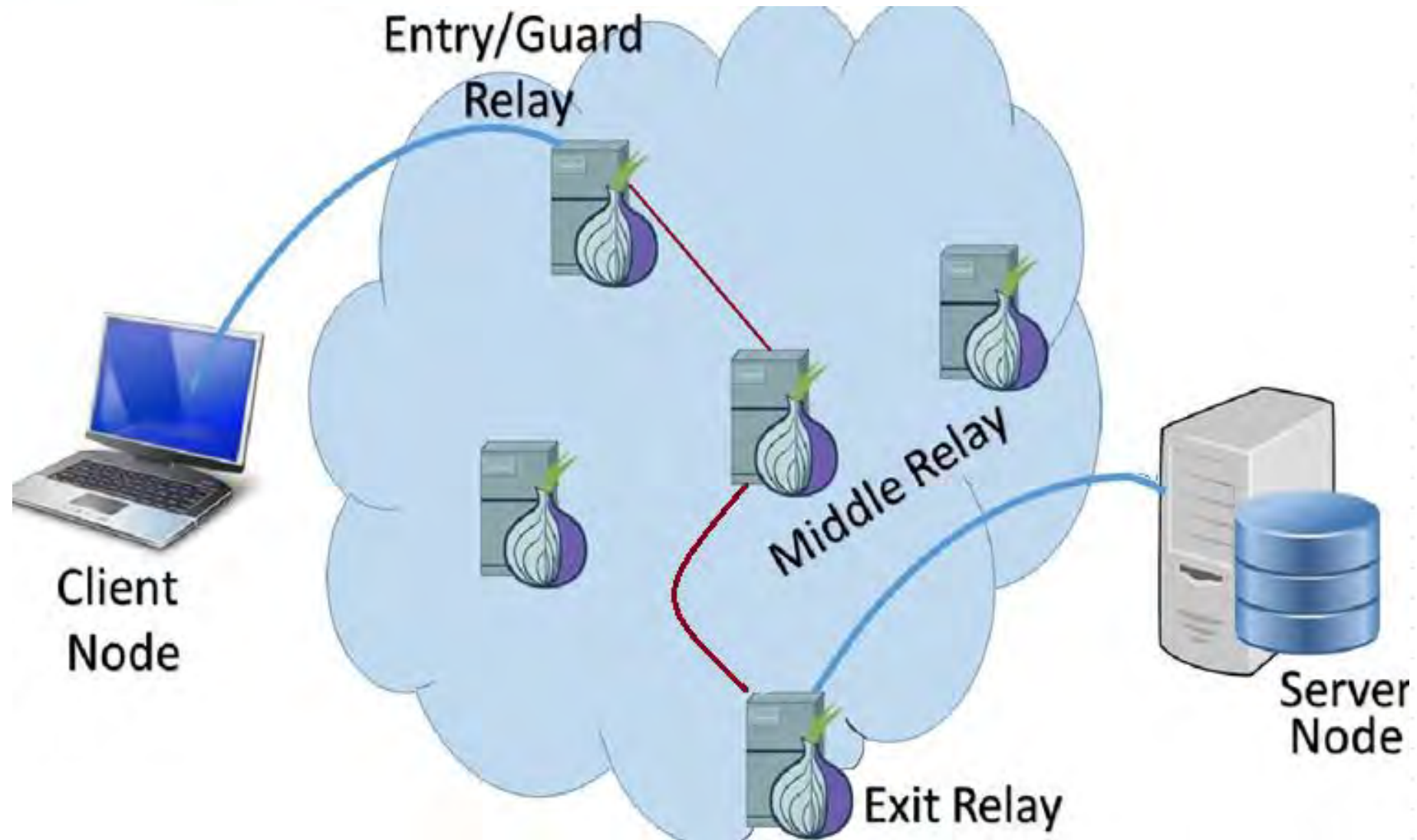
- What is Tor and how it works
 - Privacy and Safety with Tor
 - Hackers & Nation States all love Tor



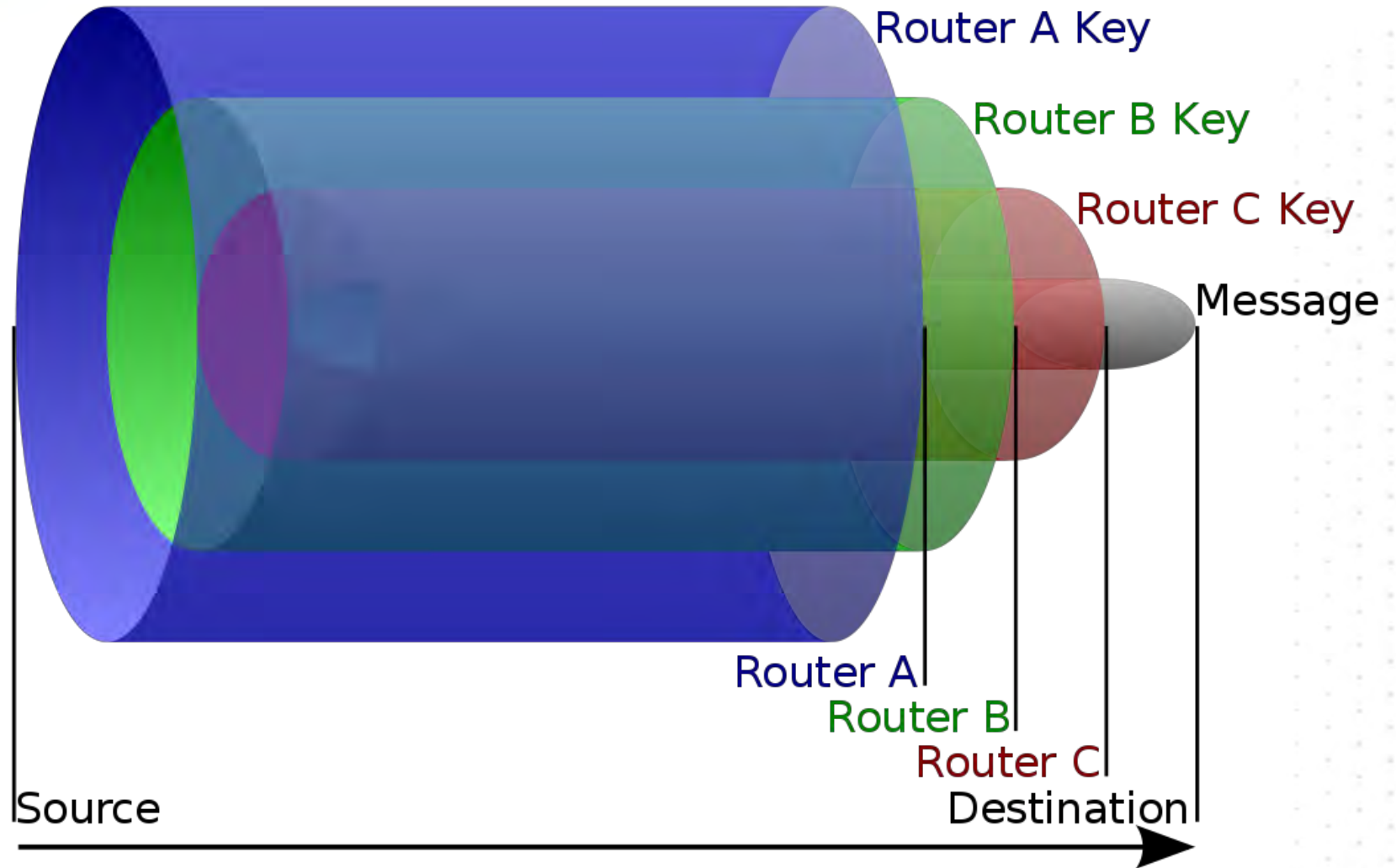
A black and white graphic with green text and a green onion icon. The text reads "USE A MASK, USE TOR." in large, bold, white letters. Below this, it says "Resist the surveillance pandemic." in white. Underneath that, in smaller white text, it says "Your donation will be matched by Friends of Tor." At the bottom, there is a green button with the text "Donate Now" in white. To the right of the text is a green onion icon, which is the symbol for Tor. The background is black with some faint green lines and a green onion icon.



Tor Traffic Flow



What is Onion Routing



TOR network?

Exit Node: Sniff credentials for use in attacks - if you forget you are on TOR and login to something without Encryption or forced to http –(non SSL/TLS) such as email, banks, personal websites, systems, blogs, you just gave them your credentials.

Capture sensitive information - Hackers love gaining access to systems in which they can linger and learn things, the TOR network makes it easy for those curious as to what people are doing on the Internet

Capture health-care and financial information - Note that health-care information is selling for more on the dark web than credit card data.

Stealing financial information such as bitcoin wallets allows the hackers to fund more campaigns.

Nation States uses ToR to be able to steal proprietary corporate information to compete on the world markets and gain competitive advantage.

To communicate securely without being detected by Governments, Suppression or law enforcement

Currency of choice is BITCOIN/Cryptocurrency

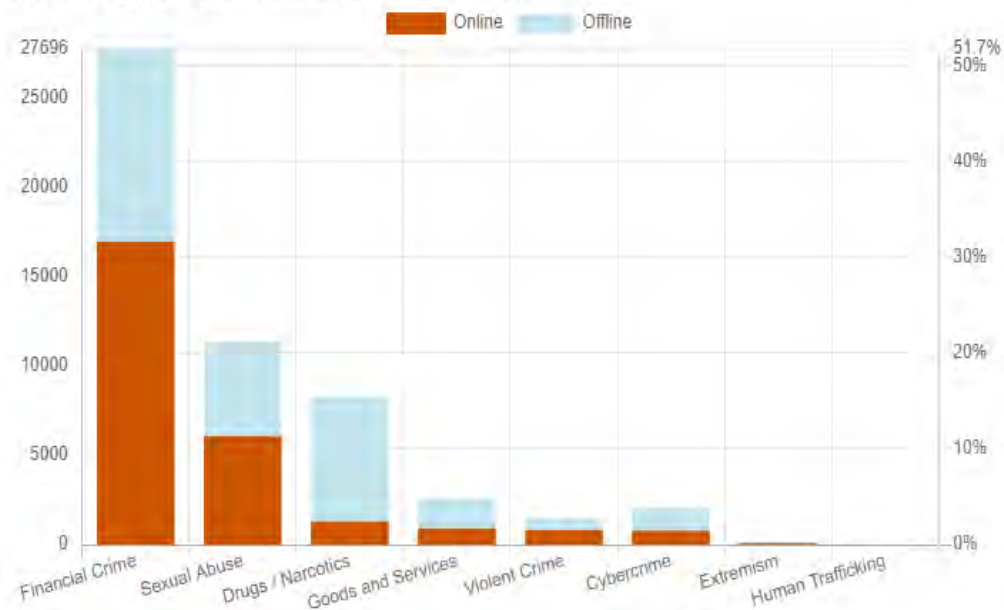


Anonymity on the Dark Web

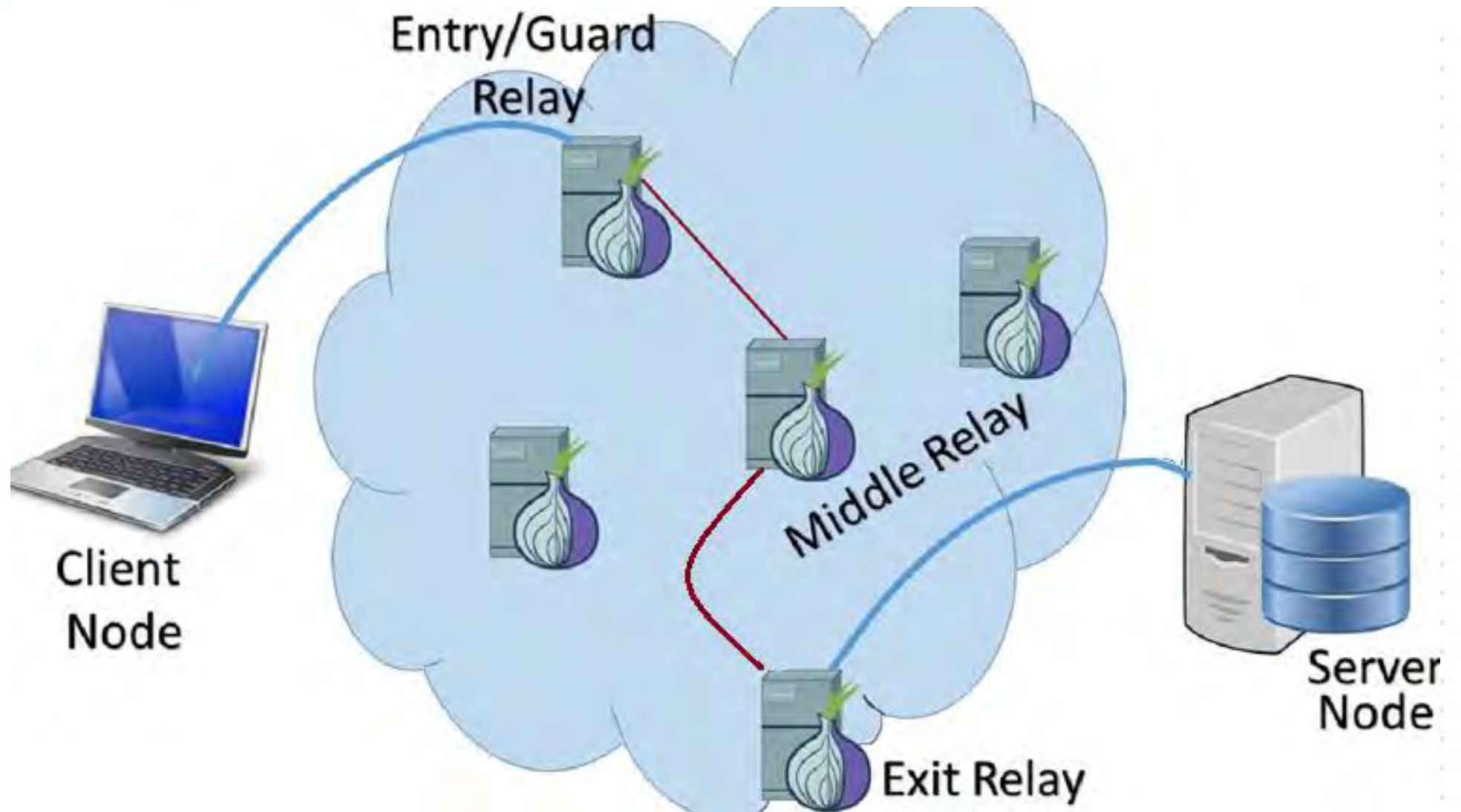
The Dark Web provides some anonymity, but not complete. We are not going to show you how to be an 31337 Hax0r and avoid detection completely, just understand there are always ways to track you.

This course is not intended as a guide to finding illegal items. There are many methods to decloak users, even the 'browser' fingerprinting method can deanonymize you.

Abuse Type Distribution over Domains



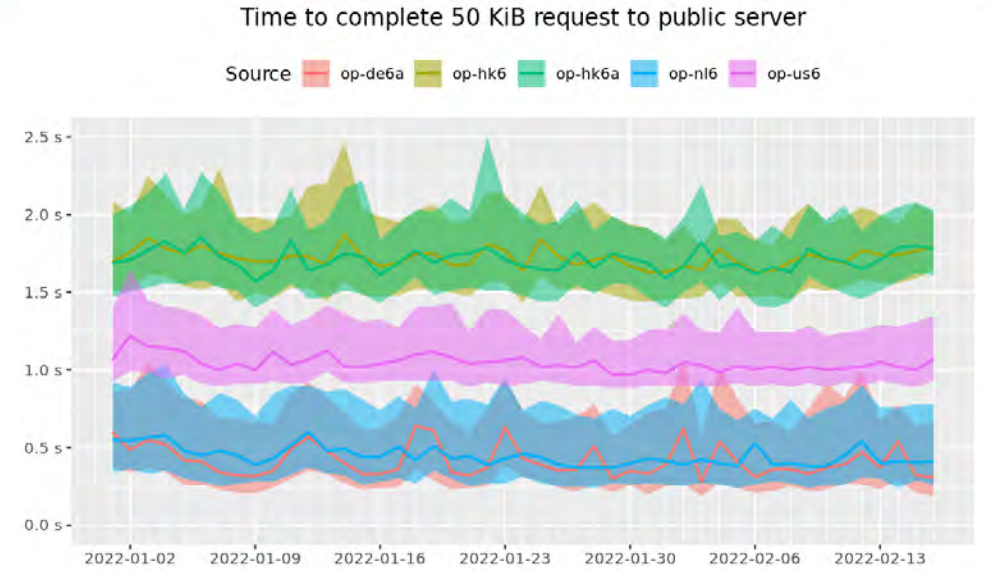
Middle Relays



<https://torflow.uncharted.software/>



<https://metrics.torproject.org/>



<https://hackertarget.com/tor-exit-node-visualization/>

<https://nyx.torproject.org/>

Terminal window showing system status and network events. The top line displays system information: 'arm - odin (Linux 2.6.28-18-generic) Tor 0.2.1.19 (unknown)'. Below this, it shows CPU usage (0.6%), memory usage (49 MB), and uptime (10-22:26:36). A section for bandwidth shows 'Downloaded (586 bytes/sec - avg: 13.2 KB/sec, total: 11.8 GB):' and 'Uploaded (586 bytes/sec - avg: 13.3 KB/sec, total: 11.9 GB):'. The bottom section shows network events, including 'router pick published address ({}): Could not determine our address locally. Checking if directory headers provide any hints.'

Map showing exit nodes found in Canada. A text box lists the following providers and their counts: Canada (Exit Nodes Found: 44). B2 Net Solutions Inc. (1), Choopa. LLC (1), Concorde inc. (1), Hurricane Electric LLC (1), Priority Colo Inc (1), University of Waterloo (1), WestConnect Communications (1), Linode. LLC (2), Hextet Systems (6), and OVH SAS (29).

<https://dnstats.net/>



Relay Search

Details for: **xkcd**

Configuration

Nickname

xkcd

OR Addresses

144.76.223.240:9001
[2a01:4f8:201:1e6::2]:9001

Uptime

27 days 5 hours 38 minutes and 24 seconds

Flags

Fast Guard HSDir Running Stable V2Dir Valid

Additional Flags

ReachableIPv6

Host Name

mail.gw90.de

Country

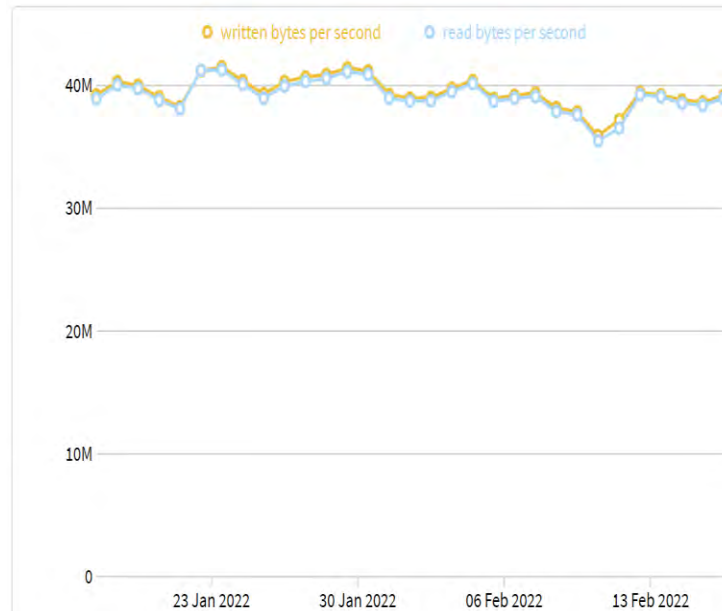
Germany

Advertised Bandwidth

62.65 MiB/s

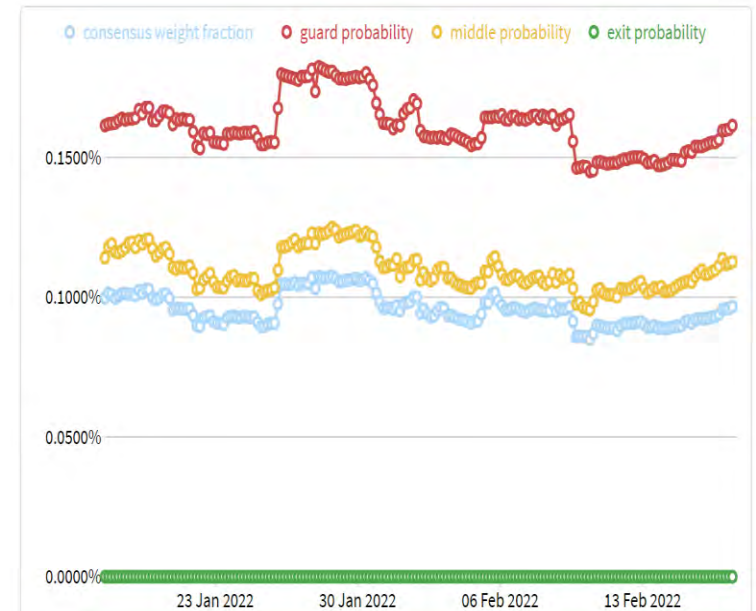
<https://metrics.torproject.org/>

1 Month 6 Months 1 Year 5 Years



1 Month graph

Save Graph



1 Month graph

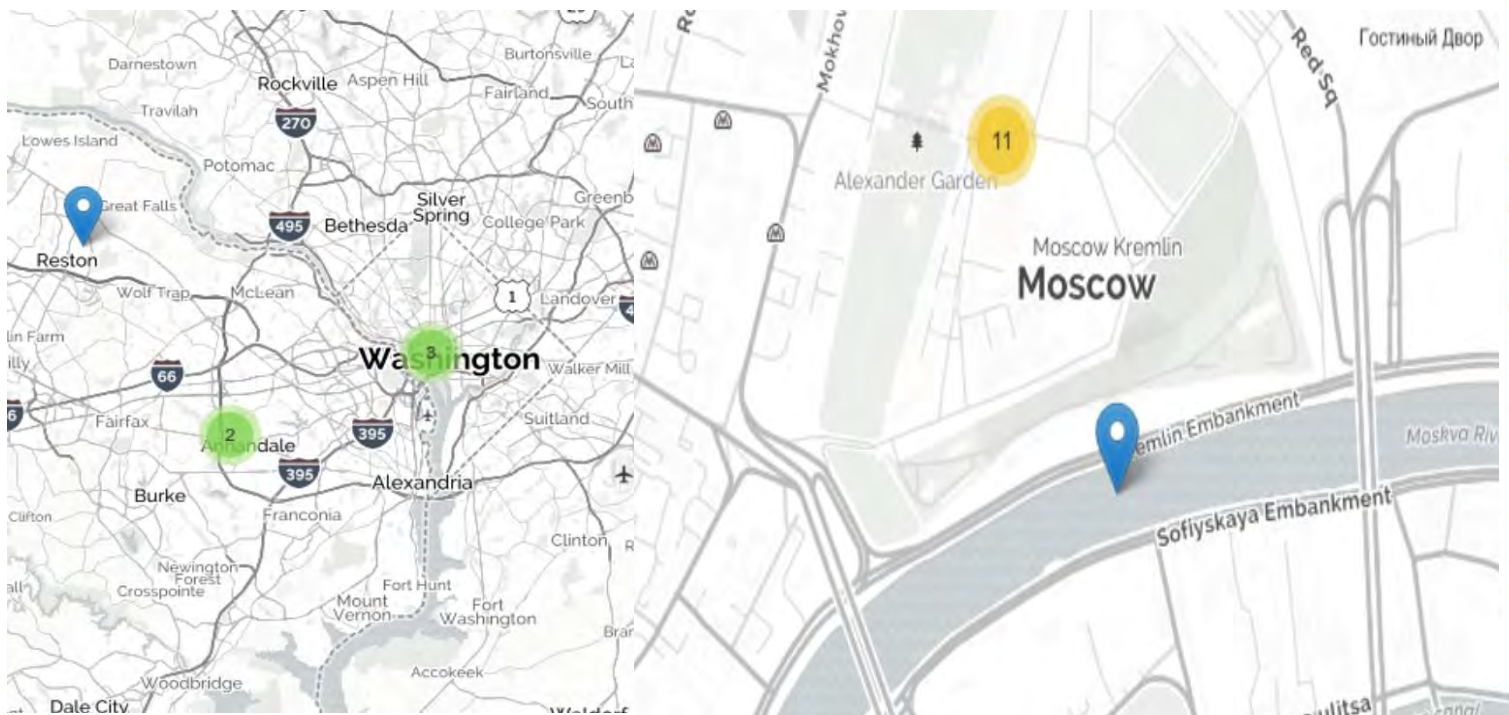
Save Graph



Surveilling Tor

A wide range of people use Tor, including journalists, human rights activists, soldiers, governments, criminals, and terrorists.

Like all low-latency anonymity networks, Tor cannot and does not attempt to protect against monitoring of traffic at the boundaries of the Tor network (i.e., the traffic entering and exiting the network). While Tor does provide protection against traffic analysis, it cannot prevent traffic confirmation, called end-to-end correlation.



A mysterious threat actor is running hundreds of malicious Tor relays

- Security researcher claims to have identified threat actor running thousands of malicious servers.
- Researchers claims the attacker may be trying to deanonymize and identify Tor users.
- Evidence suggests the attacker, tracked as KAX17, is sophisticated and well-resourced.
- The Tor Project has removed hundreds of KAX17 servers in October and November 2021.

Since at least 2017, a mysterious threat actor has run thousands of malicious servers in entry, middle, and exit positions of the Tor network in what a security researcher has described as an attempt to deanonymize Tor users.

Tracked as **KAX17**, the threat actor ran at its peak more than 900 malicious servers part of the Tor network, which typically tends to hover around a **daily total of up to 9,000-10,000**.

Some of these servers work as entry points (guards), others as middle relays, and others as exit points from the Tor network.




Even clicking on a Child Pornography/Exploitation links or a Red Room links in some Countries is illegal Including the USA.

Do Not Actively search for CP/RR at any time.

“Intent to View”




We crowdsource OSINT to help find missing people.
Become a Part of the Solution

Trace Labs is a nonprofit organization whose mission is to accelerate the family reunification of missing persons while training members in the tradecraft of open source intelligence (OSINT).

Join Trace Labs Discord - <https://discord.gg/tracelabs>

<https://www.tracelabs.org/initiatives/osint-vm>





Even visiting a website with Child Pornography **cp** could land you in trouble, on the radar – potentially in Jail, and potentially a record as a pedophile.

1. Even if you are LE, unless under an official assignment
2. Even if you say you are researching or writing a paper
3. Even if you hate the bad guys and want to report them
4. Even if you are told by someone to do it



YOU SHOULD NOT



Trigger Warning & Offensive Materials

Murder for Hire

Drugs

Weapons

Rape

Porn

Child Porn (cp)

Child Exploitation(ce)

Sexual Abuse

Sexual Content

Human Trafficking

Death

Suicide

Naked/Porn images

Voyeurism

Hackers for Hire

Carders/Accounts

Human Body Parts

Red Room (rr) Content

Illegal Classified Materials

Stolen Bank Accounts

Fake persona' & ID's

Counterfeit Products

Cracked software

Illegal Digital goods

Terrorism

Extremists

Cameras, Spying

illegal photos/videos

Bombs and IED's

Illegal hacking tools

Hacking Forums

Special VPN Access

Fake/Stolen Passports

Brothels (sex workers)

Virtual Adult Shows

Escrow Services

Suicide & Crisis Lifeline at 988 or 1-800-273-TALK (8255).



- Murder
- Rape
- Sexibition
- Mutilation
- Torture
- Dismemberment
- Chat

Red Room

There are 5 days 2 hours 36 min left

And You Could Be A Spectator!

Take Part In This Once-in-a-Lifetime Experience

The remaining still access points:

Acces Type:

SPECTATOR

You can only watch

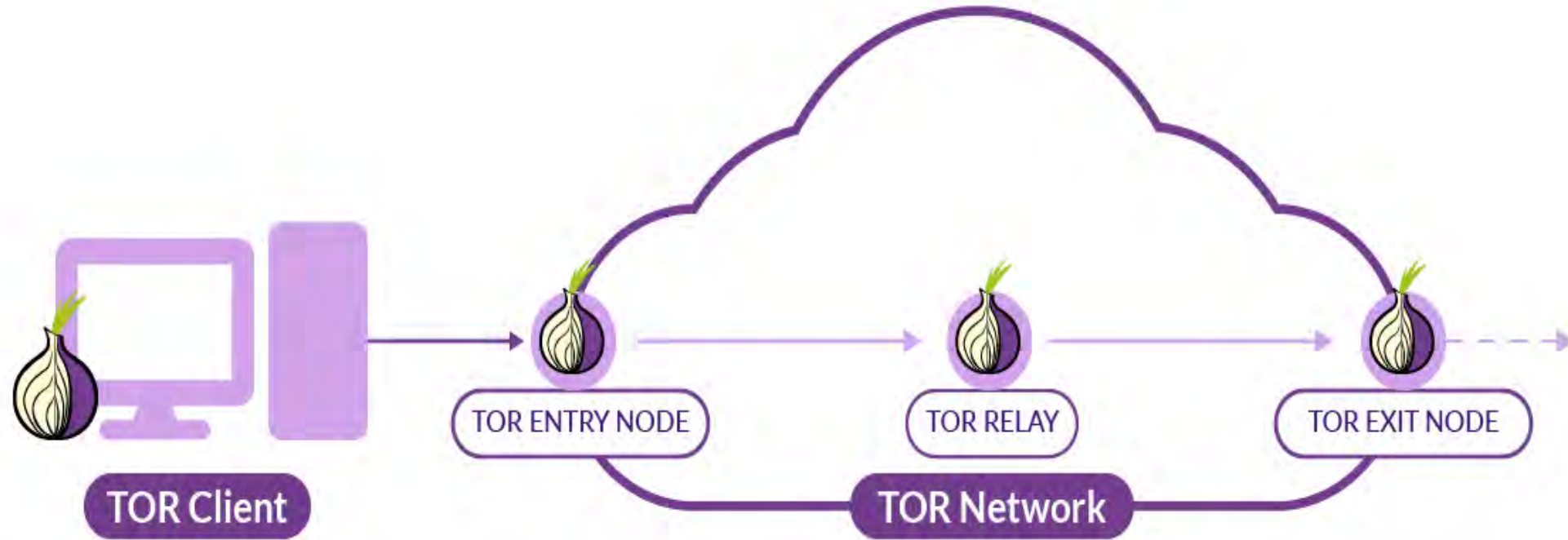
Red Room

JOIN

or

LEAVE

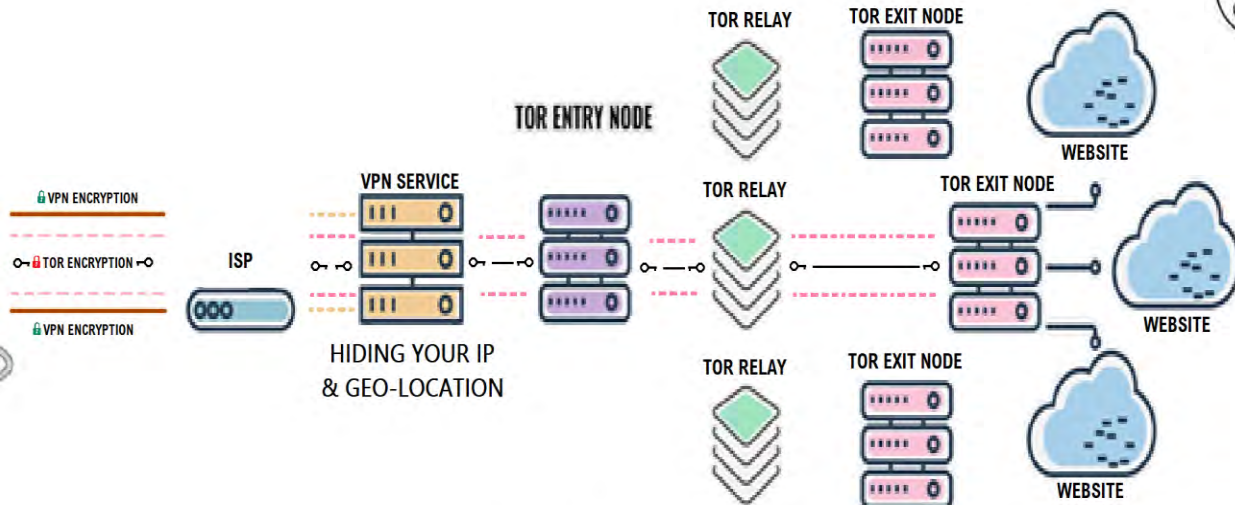
The Basics of Tor





Using Tor on Windows, Mac and Linux

- ✓ Build a Linux Virtual Machine dedicated to this activity
- ✓ Purchase or Build a VPN Service that has a no-logging policy
- ✓ Setup and configure the VPN Service before you install Tor/Tor Browser
- ✓ Ensure you have the VPN ON and operation prior to the Setup of Tor
- ✓ Download and setup the Tor Browser/Tor Service for your Operating System
- ✓ Optionally setup a Cloud Virtual Machine for private VPN access



Exercise 2

LAB 1 & 2



Virtual Cloud Based Compute

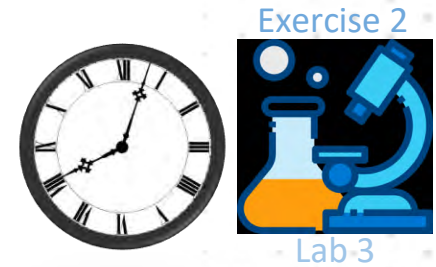
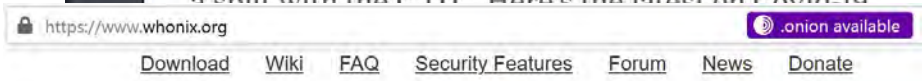
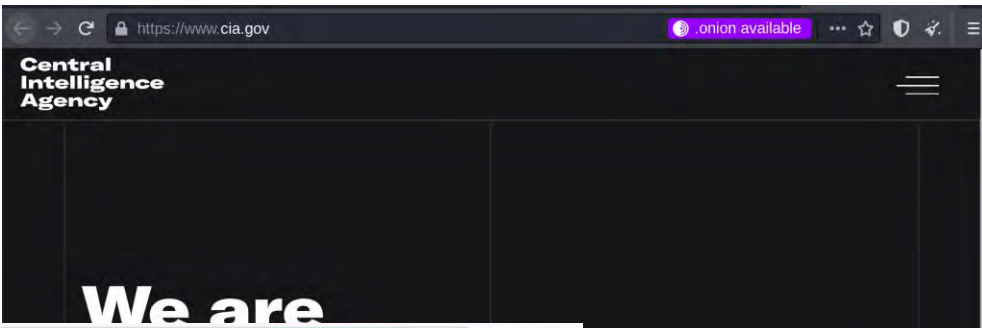
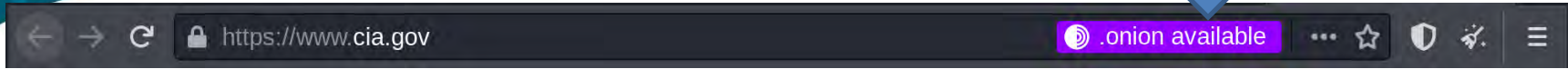
Configure a cloud virtual machine or desktop using providers such as:

- Amazon Workspaces (<https://aws.amazon.com/workspaces/>)
- Google Cloud (<https://cloud.google.com/compute>)
- Microsoft Azure VDI (<https://azure.microsoft.com/en-au/free/virtual-machines>)
- Tencent & Alibaba Cloud Systems - <https://us.alibabacloud.com/>

The logo for Alibaba Cloud, featuring an orange icon of a stylized 'A' with a right-pointing arrow, followed by the text 'Alibaba Cloud' in orange.The logo for Amazon Web Services (AWS), featuring the word 'aws' in a lowercase, sans-serif font with a yellow curved arrow underneath it.The logo for Google Cloud, featuring the multi-colored Google Cloud icon (a stylized 'G' with red, yellow, blue, and green) followed by the text 'Google Cloud' in grey.The logo for Tencent Cloud, featuring a blue icon of a stylized cloud with a white outline, followed by the text 'Tencent Cloud' in blue.The logo for Oracle Cloud Infrastructure, featuring the word 'ORACLE' in red, uppercase letters, with 'Cloud Infrastructure' in black, lowercase letters below it.The logo for Microsoft Azure, featuring a square icon divided into four colored quadrants (red, green, blue, yellow) followed by the text 'Microsoft Azure' in black.



.Onion Browser Aware Websites:



Creative Dark Web Vendors

AlphaBay Market

Home / Fraud / Accounts & Bank Drops / UBER Account Login Profiles - Worldwide Taxi Service

Listing Options

- Contact Seller
- Add to Favorites
- Report Listing

Market Categories

- Fraud: 766
- Drugs & Chemicals: 1250
- Guides & Tutorials: 316
- Counterfeit Items: 64
- Digital Products: 199
- Jewels & Gold: 7
- Weapons: 51
- Carded Items: 38
- Services: 126
- Other Listings: 75

Search Options

Search terms:

Listing type:

UBER Account Login Profiles - Worldwide Taxi Service

The format they will be delivered in will be: Live | 74.192.97.98.28117 | James Kirby | Uber Riders | Visa [052017] | [CRE:399] | I will guarantee and live ONLY. Discounts on bulk purchases. Thanks ThinkingForward

Sold by ThinkingForward - # sold since Mar 21, 2015

| Product class | Features | Origin country | Ships to |
|---------------|-----------|----------------|-----------|
| Digital goods | Unlimited | | Worldwide |
| Ends in | Never | | |

Random - 1 days - USD +0.00

Purchase price: USD 5.00

Qty: 1 [Buy Now](#)

5.00 USD

Description | Bids | Feedback

Listing Feedback

| Buyer | Date | Time | Comment |
|-------|----------------|-------|-----------------------------|
| u1y | March 26, 2015 | 21:50 | Fast and reliable as always |
| u1m | March 26, 2015 | 06:58 | quick and pro thanks mate |
| u1y | March 26, 2015 | 00:47 | |

amazonalixuydfexvh4w5xifzk74pupijdaqtgfv24rvmlnhkdfixqd.onion/all-categories/

TOR amazon

Departments

- Guns
- Drugs
- Hacking
- Financial
- Documents
- Electronics
- Medicaments

FREE DELIVERY
Free delivery on all orders over \$30

ESCROW ORDERS
Escrow by default on all orders

add to bookmark

SPOOKY SAVINGS

5% OFF ALL ORDERS

FREE DELIVERY
On all orders over \$30

NEED HELP? TORAMAZON@ONIONMAIL.ORG
Mail us to get assistance

MONEY BACK GUARANTEE
Full buyer protection no questions asked



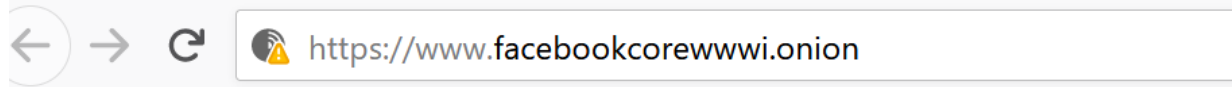
Tor v2 & v3 Address Types:

Version 2

<http://helixthunkrogtkf.onion/>

Onion Land v3

<http://3bbad7fauom4d6sgppalyqddsqb5u5p56b5k5uk2zxsy3d6ey2jobad.onion/>



Facebook over Tor has moved

Facebook over Tor has moved to a new onion service.

Visit facebookwkhpilnemxj7asaniu7vnjjbiltxjqh3mhbsg7kx5tfyd.onion.

For more information visit facebook.com/facebookcorewwi.

Lets get one thing straight its impossible to scan* the Dark Web, there are 1,208,925,819,614,629,174,706,176 site addresses on the "Tor" dark web

When you browse The Onion Service, Tor Browser displays various onion icons in the address bar to indicate the safety of the current web page.



The Onion Service is served over HTTP, or HTTPS with a CA-Issued certificate.
The Onion Service is served over HTTPS with a Self-Signed certificate.



The Onion Service is served with a script from an unsecured URL.



The Onion Service is served over HTTPS with an expired certificate.

The Onion Service is served over HTTPS with an invalid domain.

The Onion Service is served in a mixed form over an unsecured URL.

Tor v3 Addressing

Addresses in the Onion TLD are generally opaque, non-mnemonic, alpha-numerical strings which are automatically generated based on a **public key** when an onion service is configured.

The old version v2 addresses were 16 characters long. Version v3 addresses are 56 characters long. Version 3 its a 256-bit ed25519 public key along with a version number and a checksum of the key and version number

Only combinations of 56 base32 characters that are correctly encoded ed25519 public key, a checksum, and v3 are valid version 3 addresses. More details can be found here:

<https://ed25519.cr.yo.to/>

Version 2 Address - <http://helixthunkrogtkf.onion/>

Version 3 Address - <http://2fd6cemt4gmccflhm6imvdfvli3nf7zn6rfrwpsy7uhxrgbypvwf5fad.onion/>

Finding Active Dark Web Sites

<https://www.reddit.com/r/deepweb/>

<https://www.reddit.com/r/darknet/>

<https://www.darkweblist.com/>

<https://thedeepsearches.com>

V3 addressing:

<http://2fd6cemt4gmccflhm6imvdfvli3nf7zn6rfrwpsy7uhxrgbypvwf5fad.onion/>

<http://phobosxilamwcg75xt22id7aywkzol6q6rfl2flipcqoc4e4ahima5id.onion/>

**For reference only, not a recommendation*

Phobos

Dumps

SEARCH

About 1850 results (0.092 seconds)

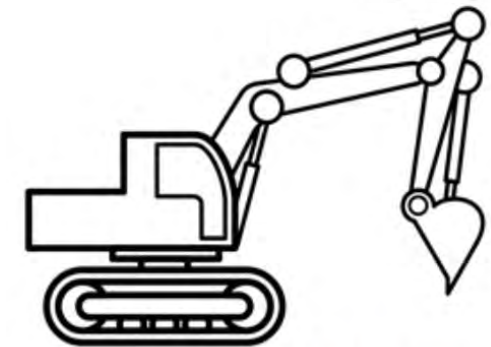
CARDS DUMPS PIN CVV - MONEY FROM THE CARD TO THE BTC WALLET

<http://h5uaeears3fnvfyhikmcueccfxahudr5ecji22xghzxc3uvvpzxfwghid.onion/>
...confirmed card Italy \$ 82 UZJPULID 788 EUR Personal Yes (confirmed) France \$ 105
E-mail address: **DUMPS** CARDS Choose an card the list below if you want to receive the details via email. Click here if you...

Dumps Market

<http://dumpsmavzqpag5xvp57xb7lgrdsjmjllsgxcvskrskebltjezsukad.onion/>
DUMPS MARKET CONTACT INFO ABOUT SHOP DUMPS MARKET GIVES YOU AN OPPORTUNITY TO BUY CREDIT CARDS, GIFT CARDS...

[Dumps Market](#) · [Dumps Market](#) · [Dumps Market](#)



EXCAVATOR

"No javascript. Safe search. We don't track you."

Don't Shoot your Organization

Pages (4): 1 2 3 4 Next »

BANORTE 10,959,629 Entries

by pompompurin - Monday August 8, 2022 at 01:18 PM

[Owner] pompompurin



Bossman

ADMINISTRATOR

Posts: 1,805
Threads: 221
Joined: Mar 2022
Reputation: 4,303

August 8, 2022, 01:18 PM

#1

I bought this data to leak (With permission from the seller) because Group-IB was sending emails to me complaining about it. They also attempted to submit DMCA's against the website. Make sure to tell BANORTE that now they need to worry about the data being leaked instead of it just being sold Mr. Group-IB. Next time do not bother me

Hello!

The Group-IB team has discovered a resource containing a fraudulent post offering to buy Grupo Financiero Banorte's leaked databases. This leads to financial and reputational risk. (banorte.com).

The post is located at the following link:
hXXps://breached[.]to/Thread-Selling-MEXICAN-BANK-BANORTE-10-959-629-LINES

Group-IB (Group-IB Ltd.) is an authorized representative of Grupo Financiero Banorte.

We ask you to remove this post containing Banorte data.

Thank you for your cooperation and prompt attention to this urgent matter.

--

Best regards,
Group-IB Digital Risk Protection
Phone: +65 3159-3798
E-Mail: drp-response@group-ib.com
Web: group-ib.com

Data included: full name, full address, phone numbers, RFC (taxes ID for Mexico), emails and balance.

Download

Trustworthy on the Darkweb?



TRUSTED **TRUSTED VENDORS LIST** **BUY NOW**
Financial, Electronics, Weapons, Documents
Counterfeited Money, Hackers and Drugs



Top Dark Market List RANK

We are still looking for the best supermarkets, unfortunately, we have been finding a lot of cheatings for a long time. The list is not up to date

List of the best Dark web Markets. The list was compiled based on the impressions of users. The list is constantly updated. Each market is described in detail. Below the description of each Market, there is also a discussion that may change its place in the ranking. Feel free to share your feelings.

TOP

| | | |
|----|---------------------------|---|
| 1. | <i>Horizon Store</i> | drzvwu6ljvqkpecivnz7rx2fldetutzrp23lxs5rs522iudywcsedjqd.onion |
| 2. | <i>Monopoly Market</i> | http://monopolydc6hvk425ov6xolmgx62q2tgown55zvhpngh75tz5xkzfyd.onion |
| 3. | <i>White House Market</i> | http://auzbdiguv5qtp37xoma3n4xfch62duxtdu4cfrwrwbxgckipd4aktxid.onion |
| 4. | <i>ASAP Market</i> | http://asap2u4pvplnkz17ecl45wajojnftja45wvovl3jrvhangeyq67ziid.onion |
| 5. | <i>Cannazon Market</i> | http://57iwpifn5xr7bim3lm4lywjuz45za4cbwusyerh362jiqnorajzh2id.onion |
| 6. | <i>ToRReZ Market</i> | http://yxuy5oau7nugw4kpb4lclrqdbixp3wvc4iuiad23ebyp2q3gx7rtrgqd.onion |

Deep & Dark Web Search

| Search engine | Index marketplaces | Index forums | Index login blocked content | Paywall blocked content | Indexed pages (estimate according to the site statistics) | Response time (sec) | Granular filtering | Linked directory | I2P search engine |
|-------------------------|--------------------|--------------|-----------------------------|-------------------------|---|---------------------|--------------------|------------------|-------------------|
| Torch/Ahima | Yes | Yes | No | No | 6M | 3 | No | No | Yes (Ahima) |
| Phobos | Yes | Yes | No | No | 10K+ | 0.5 | No | No | No |
| OnionLand Search | Yes | Yes | No | No | 10K+ | 2 | No | Yes | Yes |
| Deep Search | Yes | Yes | No | No | 225K | 3 | No | No | No |
| Tor 66 | Yes | Yes | No | No | 10K+ | 2 | No | No | No |
| Visitor | Yes | Yes | No | No | 22K | 2 | No | Yes | No |
| Hoodle | Yes | Yes | No | No | 386K | 3 | No | No | No |

Dark Markets

fxrx6qvrri4ldt7dhytdvkuakai75bpdixlmer6zrlkq34rpcqpyqd.onion/#product

SHOP CARD

HOME PRODUCT PRICE SHIPPING FORUM FAQ CONTACT

Prepaid Credit Card | WESTERN UNION | PAYPAL

Since our traffic is significantly increased and our supply is limited we changed the prices slightly. To buy cards simply send the amount of cards/shipping type and your name/shipping address. We only deal with chipped cards. Cards are 100% secure and working! Guaranteed balance of each card is 3500\$ We are only accepting bitcoin for payment. Free shipping worldwide! Express shipping only with tracking number.

All transactions pass through the Escrow service. This is how normal credit card processing works, and it provides the buyer with a level of protection because they can dispute a transaction that went wrong.

You want to sell hacked accounts? Contact us if you can sell hacked accounts or dumps on a regular basis.

**For reference only, not a recommendation*

gnyjbvkhiohdp6vnrxt06myffpgsyrfqwpy7jgvpus24kpuprxiiyqd.onion

OPIOIDS ADHD BENZOS

Dr. Feelgood

Search... All Categories

HOME PAGE SHOP MY ACCOUNT CHECKOUT CART

We sell

- MASTER CARD
- VISA
- AMERICAN EXPRESS
- CARDS

- PAYPAL
- PAYPAL

zhxkkqdjuf7vknzqo5hie2nfp7d3zgqlehdiiyigphidrslyktmfo6ad.onion

Imperial SINCE 2014

VISA MasterCard PayPal WESTERN UNION Gift Card

FAQ Proofs Reviews

Best Financial Market

Prepaid / Cloned / Gift Cards and Money Transfers via PayPal or Western Union

See Products

zhxkkqdjuf7vknzqo...onion Verified by Tor HIDDEN WIKI DEEP DOT WEB The Hidden Wiki reddit

WE DO NOT HAVE ANY LISTINGS ON DARK MARKETS. IF YOU SEE SOMEONE CALLED 'IMPERIAL MARKET' THERE, THEY ARE PROBABLY SCAMMERS WHO USE OUR NAME. BE CAREFUL!

All transactions are monitored [Safe Escrow](#)

LSD (3)

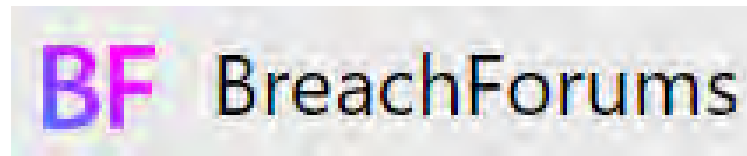
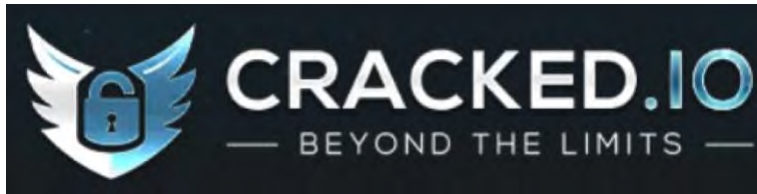
YOU ARE ANONYMOUS!*

Anonymous! Anonymous! Anonymous!

Read the fine print. You are actually not anonymous. *Not Really

We log your...

Hacker Forums




Escrow services



You can access to secMail through the following Tor addresses:
New v3 address: <http://secmail63sex4dfv6h2nsrbmfz...>
Classic address: <http://secmailw453j7piv.onion>

→ ↻ yrrqzjkkf5l4v4ik.onion 80% ☆


SAFESCROW

WE DEFINE
TRUST

Our platform allows vendors and customers to confidently work together.
We handle store integration, so all transactions run through escrow. If
there are any issues in the sales process, we make sure it gets handled right.

Bitcoin Mixers

Blockchain.com Search Blockchain, Transactions, Addresses and Blocks

Home 0.42 ▼7.44% USD Coin/USD 1.01 ▲0.40% Cardano/USD 0.36 ▼4.44% Staked Ether/USD 1,847.96 ▼3.89% Solana/USD 20.61 ▼8.64% Arbitrum/USD

Prices Charts NFTs

Sponsored: Win up to 10 BTC! VPN Friendly & NO KYC Casino [Play Now](#) [Get Your Free Spin](#) [Play Slots & Win!](#)

USD Bitcoin BTC \$27,504.26 -6.91% -2,041.48

Latest Blocks Bitcoin 788,832 • Binance Pool 08 May 2023 • 03:25:42 GMT-5 3,755 Txns • 1.60 Mh

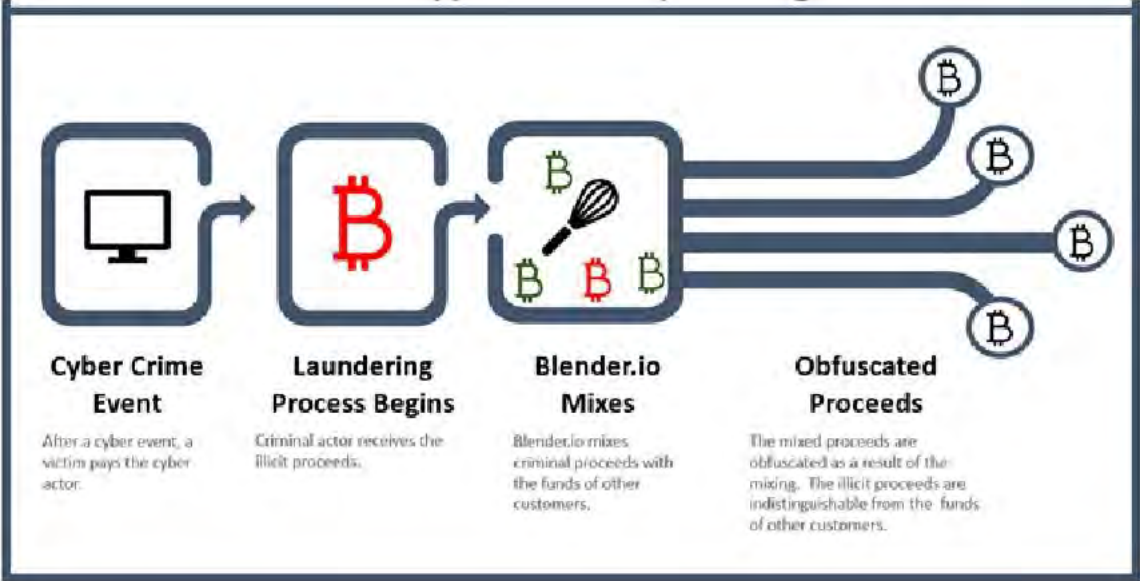
U.S. Treasury Issues First-Ever Sanctions on a Virtual Currency Mixer, Targets DPRK Cyber Threats



May 6, 2022

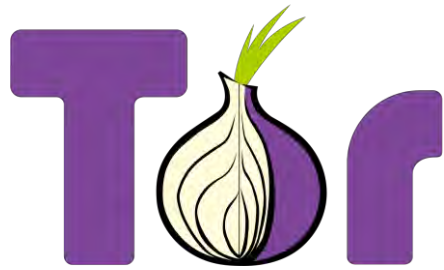
Additional Lazarus Group Virtual Wallet Addresses Identified

WASHINGTON – Today, the U.S. Department of the Treasury’s Office of Foreign Assets Control (OFAC) sanctioned virtual currency mixer Blender.io (Blender), which is used by the Democratic People’s Republic of Korea (DPRK) to support its malicious cyber activities and...



Reputation, Intel, Third Party Services

- Should you invest in a Dark Web Search services
- Should you purchase Darknets Intelligence platform Access
- Should you have your team searching the Darknets?



ZeroNet

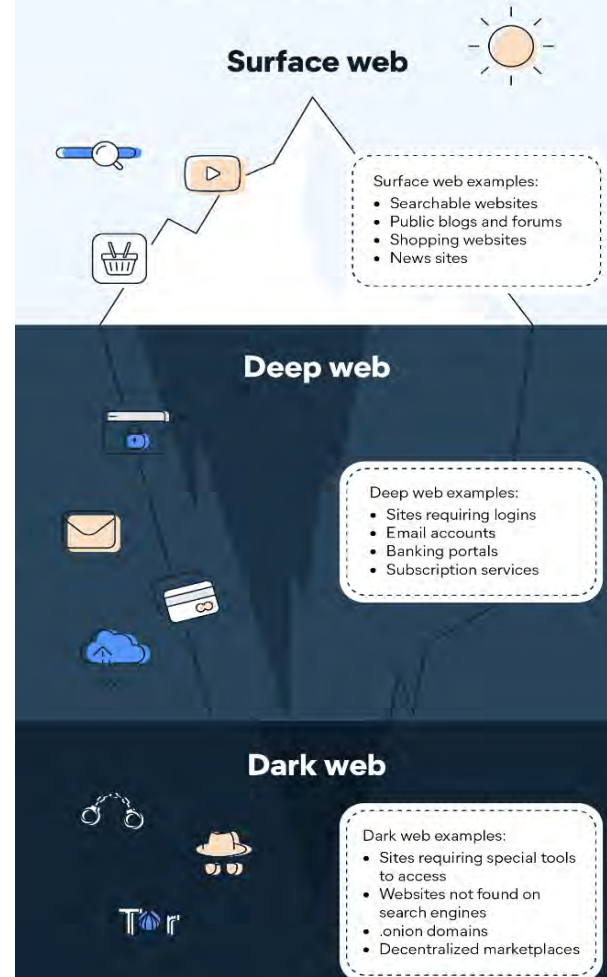


Telegram



What Is the Dark Web?

The dark web is the part of the deep web that can be accessed only with special tools or software like Tor.



Buying on the dark web?

You are on the menu!



you



Refund Fraud-as-a-Service

Important Threads

- ★ REFUND GOD ★ FAST REPLIES ★ 8 YEARS EXPERIENCE ★ \$2000+ LIMITS**
 ★ USA ★ CANADA ★ WORLD ★ (Pages: 1 2 3 4 ... 6)
 Copperhorse 3 months ago
- + 8%-20% WORLDWIDE REFUNDS | 100% SR | NL SPECIALIST | FAST SUPPORT | VOUCHERED | 100+ STORES** (Pages: 1 2 3 4 ... 26)
 Money101 2 years ago
- REFUNDING TEAM | EU SPECIAL | 2000+ ORDERS | STARTING -10% | VOUCHERED | FAST SUPPORT** (Pages: 1 2 3 4 ... 18)
 instaplug 1 year ago
- SUPREME REDACTED IN TRANSIT REFUNDS REDACTED REFUND SPECIALIST**
 INSTANTS TOP REF (Pages: 1 2 3 4 ... 21)
 DoritoZlime 1 year ago
- REKK'S REFUNDS | 20000+ CUSTOMERS | 10K+ VOUCHES GROUP | TELEGRAM GROUP | ONLINE 24/7** (Pages: 1 2 3 4 ... 12)
 rekk 2 years ago
- #1 USA | CANADA | REDACTED REFUNDS | 2000+ VOUCHES | BEST CUSTOMER SUPPORT** (Pages: 1 2 3 4 ... 14)
 MrMackey 1 year ago
- REDACTED METHOD] 5% FEE STARTING REDACTED REFUNDS -BEST GERMAN REFUNDER** (Pages: 1 2 3)
 AngelJust 2 years ago

Return Rate by Retail Category

| Retail Category | Blended Return Rate ⁽¹⁾ |
|--|------------------------------------|
| Apparel | 12.2% |
| Auto Parts | 19.4% |
| Beauty | 4.3% |
| Department Stores | 11.4% |
| Drug/Pharmacies | 1.6% |
| Footwear | 9.1% |
| Hard Goods | 3.8% |
| Home Improvement | 11.5% |
| Housewares | 11.5% |
| Sporting Goods | 7.6% |
| Survey Average ^{(2) (3)} | 10.6% |

FraudBox
#1 Private Method Hub

- 100% EXCLUSIVE
- 50,000+ METHODS & RESOURCES
- CUSTOM TOOLS

Start now and get access to exclusive content, learn at your own pace on mobile or desktop.

Library thousands of HQ resources and methods.

Access to custom serial number generators, receipt generators and more.

[Create Account](#) [Go to Store](#)

Summary of Returns and Return Fraud

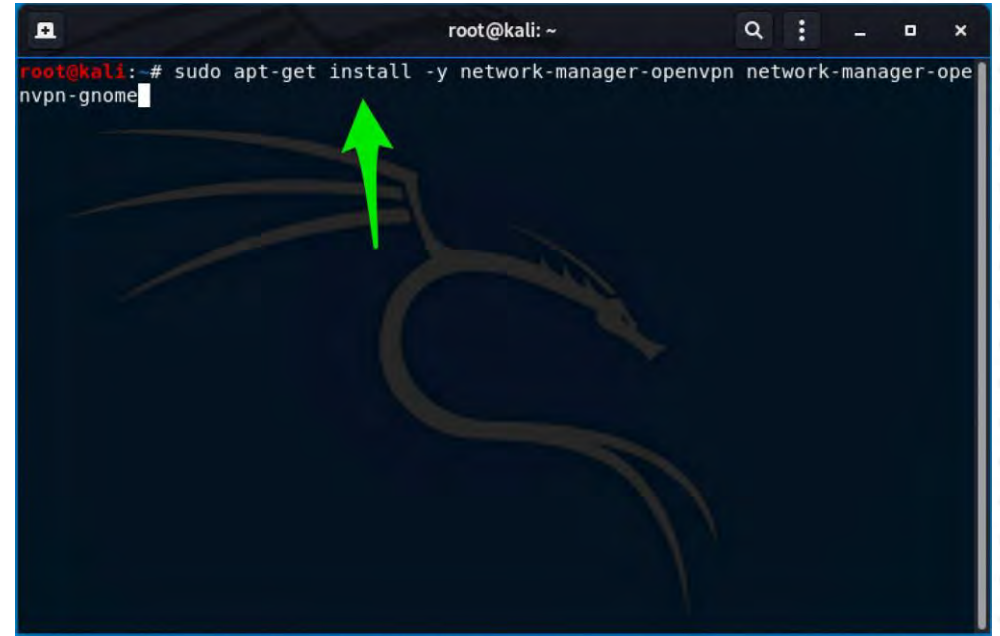
| Metric | Average | Retail Industry |
|---|---------|---------------------|
| NRF 2020 US retail industry sales ⁽¹⁾⁽²⁾ (in-store and online) | 100% | \$4,037,825,212,000 |
| Total amount of returns | 10.6% | \$428,009,472,472 |
| Total amount of fraudulent returns | 5.9% | \$25,252,558,876 |
| Non-receipted returns | 17.8% | \$76,185,686,100 |
| Non-receipted return fraud | 16.6% | \$12,646,823,893 |
| Receipted returns | 82.2% | \$351,823,786,372 |
| Receipted return fraud ⁽³⁾ | 3.6% | \$12,605,734,983 |

Using a Commercial VPN Service

There are hundreds of VPN Providers out there from NordVPN, ExpressVPN, PIA Private Internet Access, to IPVanish and more. There are several benefits to using a VPN, including enhanced anonymity.

Can you trust your VPN provider? Many of them say they do not log, but a study found they do.

You can also setup your own VPN Device in the cloud which we will cover later.



```
root@kali: ~  
root@kali:~# sudo apt-get install -y network-manager-openvpn network-manager-openvpn-gnome
```


A terminal window with a Kali Linux dragon logo in the background. The terminal shows the command to install network-manager-openvpn and network-manager-openvpn-gnome. A green arrow points to the end of the command line.

For now we are going to configure OpenVPN and a commercial VPN Service

The E3/L1, I will be doing for you to follow along with is for demonstration purposes only

OpenVPN & VPNBook



VPNBook news Free VPN accounts Free Web proxy

FA Free PPTP VPN \$0/mo

PPTP (point to point tunneling) is widely used since it is supported across all Microsoft Windows, Linux, Apple, Mobile and PS3 platforms. It is however easier to block and might not work if your ISP or government blocks the protocol. In that case you need to use OpenVPN, which is impossible to detect or block.

- [PL226.vpnbook.com](#)
- [DE4.vpnbook.com](#)
- [us1.vpnbook.com](#) (US VPN - optimized for fast web surfing; no p2p downloading)
- [us2.vpnbook.com](#) (US VPN - optimized for fast web surfing; no p2p downloading)
- [ca222.vpnbook.com](#) (Canada VPN - optimized for fast web surfing; no p2p downloading)
- [ca198.vpnbook.com](#) (Canada VPN - optimized for fast web surfing; no p2p downloading)
- [fr1.vpnbook.com](#) (France VPN - optimized for fast web surfing; no p2p downloading)
- [fr8.vpnbook.com](#) (France VPN - optimized for fast web surfing; no p2p downloading)
- Username: **vpnbook**
- Password: **e7x76mc**

More servers coming. Please Donate.

FA Free OpenVPN (Recommended) \$0/mo

OpenVPN is the best and most recommended open-source VPN software world-wide. It is the most secure VPN option. You need to download the open-source [OpenVPN Client](#) and our configuration and certificate bundle from the links below (use TCP if you cannot connect to UDP due to network restriction).

- [PL226 OpenVPN Certificate Bundle](#)
- [DE4 OpenVPN Certificate Bundle](#)
- [US1 OpenVPN Certificate Bundle](#) (optimized for fast web surfing; no p2p downloading)
- [US2 OpenVPN Certificate Bundle](#) (optimized for fast web surfing; no p2p downloading)
- [CA222 OpenVPN Certificate Bundle](#) (optimized for fast web surfing; no p2p downloading)
- [CA198 OpenVPN Certificate Bundle](#) (optimized for fast web surfing; no p2p downloading)
- [FR1 OpenVPN Certificate Bundle](#) (optimized for fast web surfing; no p2p downloading)
- [FR8 OpenVPN Certificate Bundle](#) (optimized for fast web surfing; no p2p downloading)
- All bundles include UDP53, UDP 25000, TCP 80, TCP 443 profile
- Username: **vpnbook**
- Password: **e7x76mc**

```
apt-get install openvpn  
openvpn --config vpnbook-pl226-udp53.ovpn
```

Username: **vpnbook**
Password: **e7x76mc**

Free – but don't use them for anything critical, and be wary of MITM notices

Exercise 3



Lab 2



Using Proxies & Proxychains

```
root@kali: ~
File Edit View Search Terminal Help
GNU nano 2.9.5 /etc/proxychains.conf

# proxychains.conf  VER 3.1
#
# HTTP, SOCKS4, SOCKS5 tunneling proxifier with DNS.
#
# The option below identifies how the ProxyList is treated.
# only one option should be uncommented at time,
# otherwise the last appearing option will be accepted
#
dynamic_chain
#
# Dynamic - Each connection will be done via chained proxies
# all proxies chained in the order as they appear in the list
# at least one proxy must be online to play in chain
# (dead proxies are skipped)
# otherwise EINTR is returned to the app
#
strict_chain
#
# Strict - Each connection will be done via chained proxies
# all proxies chained in the order as they appear in the list
# all proxies must be online to play in chain
# otherwise EINTR is returned to the app
#
random_chain
#
# Random - Each connection will be done via random proxy
# (or proxy chain, see chain_len) from the list.
# this option is good to test your IDS :)
#
# Make sense only if random_chain
#chain_len = 2

^G Get Help      ^O Write Out    ^W Where Is    ^K Cut Text     ^J Justify     ^C Cur Pos
^X Exit          ^R Read File   ^N Replace     ^U Uncut Text  ^T To Spell   ^_ Go To Line
```

Web Browser Based Proxies

SpysOne – Proxy List

apt-get install proxychains

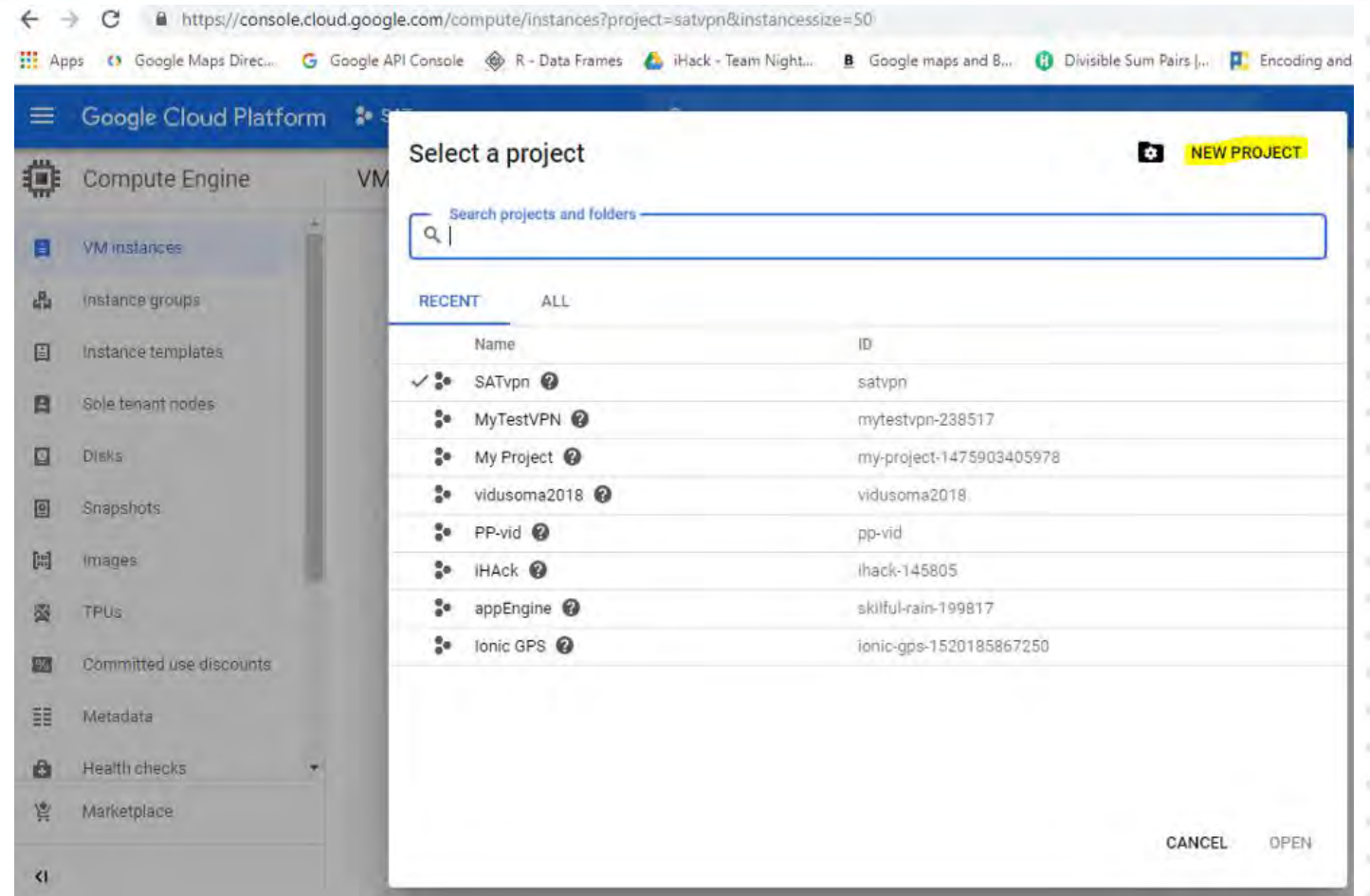
edit /etc/proxychains.conf

Exercise 4



Creating your own GCP Cloud VPN Server

Start at:
<https://console.cloud.google.com/>
and Login with your Google Account.
If you're a first time user, you can make use of the Free Tier \$300 provided by Google, you will need to create a billing account associated with a Credit/Debit card.



Exercise 5





Creating your own GCP Cloud VPN Server

Login to GCP Console

Create a new project

Project name - VPN

Setup a new google Compute Engine VM Instance

Compute Engine>VM Instances>Create>

allow HTTPS traffic under Firewall Subheading

Hostname: vpn-yours

Select Network Interfaces, click the pencil edit,

Select Standard (us-east) & Ip Forwarding On

Done

Now that all the settings are done, select Create Button

IPsec an Open Source VPN Server

Click on SSH, enter: `wget https://git.io/vpnsetup -O vpnsetup.sh && sudo \ VPN_IPSEC_PSK='secret_key' \ VPN_USER='username' \ VPN_PASSWORD='password' \ ssh vpnsetup.sh`

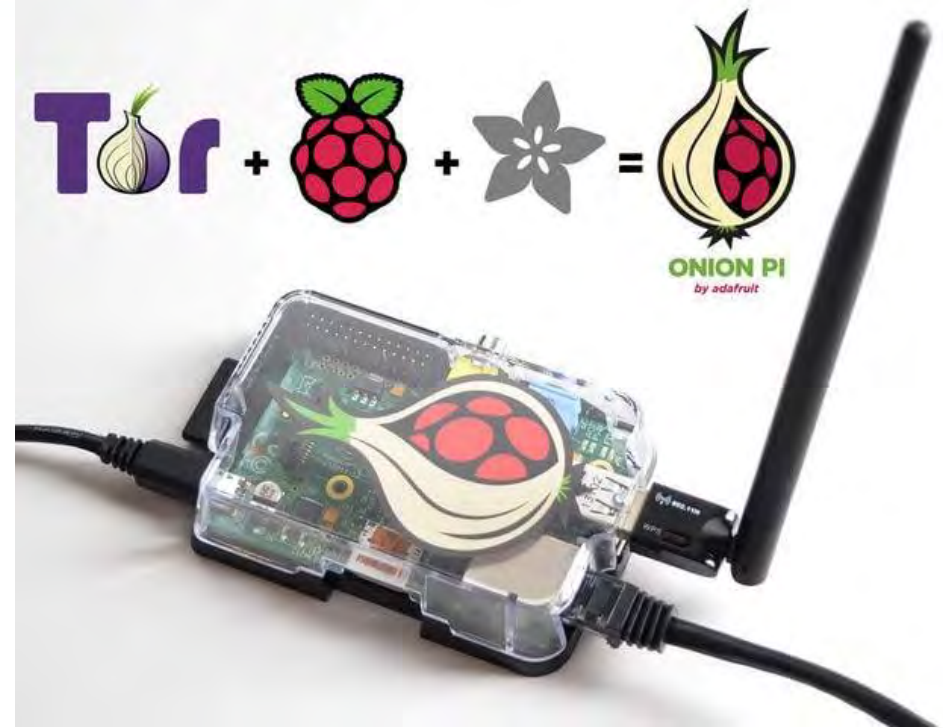
Make sure you open UDP 500 and 4500 Ports in GCE firewall rules and routes

The screenshot shows the Google Cloud Platform console interface. The top navigation bar includes 'Google Cloud Platform' and 'myVPN'. The left sidebar shows the 'Compute Engine' menu with 'VM instances' selected. The main content area displays a table of VM instances. Below the table, a terminal window shows the following output:

```
IPsec VPN server is now ready for use!  
  
Connect to your new VPN with these details:  
  
Server IP: 35.245.24.183  
IPsec PSK: 12345678912345678912  
Username: testUser  
Password: testPassword  
  
Write these down. You'll need them to connect!
```



<https://torrouters.com/>



<https://learn.adafruit.com/onion-pi/overview>



Dark Web RECON tools

Tools:

- Katana - <https://github.com/adnane-X-tebbaa/Katana>
- OnionSearch - <https://github.com/megadose/OnionSearch>
- Onionscan - <https://github.com/s-rah/onionscan>
- Onioff - <https://github.com/k4m4/onioff>
- Onion-nmap - <https://github.com/milesrichardson/docker-onion-nmap>
- Darkdump - <https://github.com/josh0xA/darkdump>
- TorBot - <https://github.com/DedSecInside/TorBot>
- TorCrawl - <https://github.com/MikeMeliz/TorCrawl.py>
- VigilantOnion - <https://github.com/andreyglauzer/VigilantOnion>
- OnionIngestor - <https://github.com/danieleperera/OnionIngestor>
- Darc - <https://github.com/JarryShaw/darc>



Search Engines:

- Ahmia Search Engine - ahmia.fi
- deepdarkCTI - <https://github.com/fastfire/deepdarkCTI>
- Dark.Fail





Tools: OnionScan

1. Remove already installed Go From a terminal:

```
sudo apt-get remove golang-go
```

```
sudo apt-get remove --auto-remove golang-go
```

2. Browse to the Go website and download <https://golang.org/> version 1.16

Linux

Linux 2.6.23 or later, Intel 64-bit processor

[go1.16.linux-amd64.tar.gz](#) (123MB)

3. Suggest you reboot after you remove the old version of Go.

4. Go to your downloads directory under your user and open a terminal window

```
tar -C /usr/local/ -xzf go1.16.linux-amd64.tar.gz
export GOROOT=/usr/local/go export
GOPATH=/root/go-workspace
PATH=$PATH:$GOROOT/bin/:$GOPATH/bin go version
```

5. Next we download Onionscan

```
go get github.com/s-rah/onionscan
```

a. Next do a "go get" for each of the below packages

```
go get golang.org/x/crypto/openpgp/packet
```

go get golang.org/x/net/proxy - For the Tor SOCKS Proxy connection

go get golang.org/x/net/html - For HTML parsing go get github.com/rwcarlsen/goexif

- For EXIF data extraction go get github.com/HouzuoGuo/tiedot/db - For crawl

database

<https://onionscan.org/>



OnionScan is a free and open source tool for investigating the Dark Web. Read more about how it works and how to use it on [GitHub](#).

Discovering the Dark Web

For all the amazing technological innovations in the anonymity and privacy space, there is always a constant threat that has no effective technological patch - human error.

Whether it is operational security leaks or software misconfiguration - most often attacks on anonymity don't come from breaking the underlying systems, but from ourselves.

OnionScan has two primary goals:

- We want to help **operators of hidden services find and fix operational security issues with their services**. We want to help them detect misconfigurations and we want to inspire a new generation of anonymity engineering projects to help make the world a more private place.
- Secondly we want to help **researchers and investigators monitor and track**

Get OnionScan 0.2

You can find download and installation instructions for OnionScan on our [Github](#)

OnionScan is also available on some Linux distributions



Exercise 6

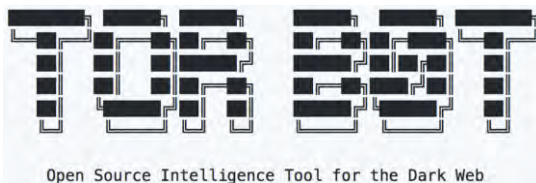




TorBot is an open-source intelligence tool developed in python. The main objective of this project is to collect open data from the deep web (aka dark web) and with the help of data mining algorithms, collect as much information as possible and produce an interactive tree graph. The interactive tree graph module will be able to display the relations of the collected intelligence data

- **Onion Crawler (.onion).(Completed)**
- **Returns Page title and address with a short description of the site.(Partially Completed)**
- **Save links to the database.(PR to be reviewed)**
- **Get emails from the site.(Completed)**
- **Save crawl info to JSON file.(Completed)**
- **Crawl custom domains.(Completed)**
- **Check if the link is live.(Completed)**
- **Built-in Updater.(Completed)**
- **TorBot GUI (In progress)**
- **Social Media integration.(not Started)**

DedSecInside / TorBot



Open Source Intelligence Tool for the Dark Web

```
docker run --link tor:tor --rm -ti dedsecinside/torbot
```

```
python3 torBot.py or use the -h/--help argument
```

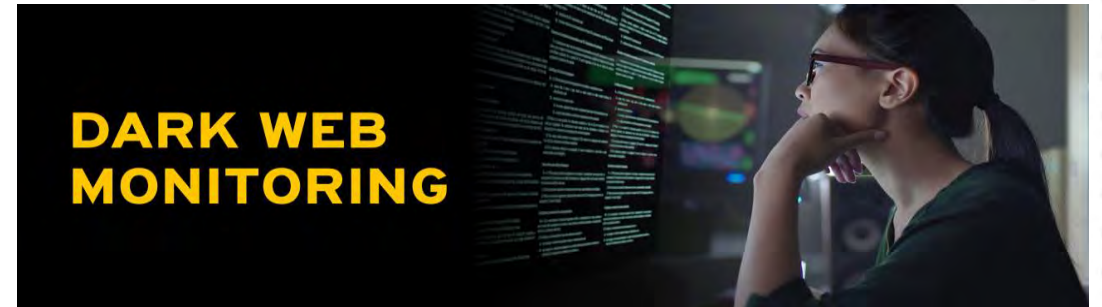
```
usage: torBot.py [-h] [-v] [--update] [-q] [-u URL] [-s] [-m] [-e EXTENSION]
                [-i]

optional arguments:
  -h, --help            Show this help message and exit
  -v, --version          Show current version of TorBot.
  --update              Update TorBot to the latest stable version
  -q, --quiet           Prevent header from displaying
  -u URL, --url URL     Specifiy a website link to crawl, currently returns links on that page
  -s, --save            Save results to a file in json format
  -m, --mail            Get e-mail addresses from the crawled sites
  -e EXTENSION, --extension EXTENSION
                        Specifiy additional website extensions to the
                        list(.com or .org etc)
  -i, --info            Info displays basic info of the scanned site (very
                        slow)`
```

Professional Dark Web Monitoring



- With dark web monitoring, you will at least know when your information is on the dark web.
- At that point, it usually has either been used or sold to other cybercriminals, but you should still take immediate action to change passwords and adjust account information for added protection.



Your information could be sold and used multiple times without you finding out.



One Minute on in the Dark

- 1000 Malicious chats on Telegram
- 220 Credit Cards are offered for sale, over two million a week
- 753 Drug related discussions
- 0.20 CVE's are mentioned, one every five minutes
- 3 suspicious IPs are shared
- 0.15 Malware links are shared
- 4 Emails are shared
- 18 Cryptocurrency transactions
- 129 Ransomware discussions





Staying Safe, OSINT in the Dark

Take the time in your research “identity” Non-Attributable

Create a “Investigative persona” aka Sock Puppet - if you plan to investigate

Create a Virtual Machine (preferably Debian based) like Ubuntu or Kali, or Cloud based.

Create a new email address - such as bob723697812@gmail.com or Protonmail

Don't use your real cell number use a phone service if required

or get a disposable phone number and/or transfer the number to google.

Obtain a commercial VPN Account or setup your own in AWS or GCP

Download Tor and the Tor Browser and install on the system

Firefox plugin's “Noscript” as well as others that turn off and limit capabilities

Enable/install configure UFW (Firewall) for Debian.

Configure proxies and proxychains where possible, use foxyproxy to manage proxies.

Ensure you and the programs you use do not collect CP/RR of any kind.

Once you have your system exactly like you want it, make a snapshot and backup.

Save each VM/Image separate for each case/investigation

Staying Safe while on the Darkweb

TOR OVER VPN

VPN CLIENT + TOR CLIENT



VPN ENCRYPTION

MIDDLE NODE

EXIT NODE



MIDDLE NODE

EXIT NODE



ISP

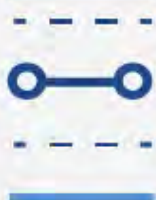
VPN SERVER

TOR ENTRY NODE

MIDDLE NODE

EXIT NODE

WEBSITE





Investigations on the dark web usually comes down to extensive research, attribution and correlation between the surface and dark web many times through information slippage. Investigations weeks and months.

<https://onion.live/>



ONION.live

HOME VERIFY MIRRORS NEWS TRUST DB LOGIN LIGHT

Top Trending

- #Sex #Kids #Loli #Video #Teen #Onion #Drugs #Adult #Free #Cards #Darkweb #Cvv #Hacking #Porno0d #Pornhub
- #Chan #Money #Xplay #Forum #Chat #Link #Bitcoin #Vendor #Deepweb #Pthc #Searchengine #Cannabis #Pornhb
- #Guns #Snapchat #Paypal #Weed #Underground #Asap #Torch #Kingdom #Bohemia #Cebulka #Ket #Alphabay #Rindexxx
- #Phobos #Hydra #Darkfox #Books #Torbox #Incognito #Cocorico #Markets #Vendor Shops #Discussion Forums #Onion Directory

#Hall of Shame

- RuTor (Russian)
- Dread Forum
- dark.fail

Finding Intel' & Dumps

NEWS BUY RULES ORDERS BILLING CHECKER SUPPORT

Activation

Registration fee: \$150
Minimum deposit: \$200
Total amount: \$350

Registration rules:
- registration is carried out on a free will;

BITCOIN USD 39510.36
USD 1
BTC
17 Feb 2022, 06:04pm



BHF.IO / .IM / .LA

https://pompur.in/

Снимаю 2FA с Binance и с других бирж

РЕДЛИНЕ @REDLINESUPPORT

Последние сообщения Новые темы Горячие темы Базы Розыгрыши Последняя активность

- Проверено [Сервис] Инсталлы ЮСА/ЕУ/Микс Мира [Service] Installs USA/EU/Mix World
- Холдеры, ICO, биржи, Админки, Обрабатываем \ Выкупаем
- Проверено сайт [AllWorldCards] Best CreditCards + CVV for best price!

<https://deepwebmarketsreview.com>



r/shanghai

Shanghai Police Data Breach

Posted by u/skripp11 10 months ago

This was brought up in another [thread](#) but I believe this important enough warrant it's own post.

About Community

r/shanghai

dread frontpage all dread

/d/DarkNetMarkets

64,633 subscribers

SUBSCRIBE

SUBMIT A POST

GET MARKET LINKS HERE!

Visit the Market Superlist Here: /post/d5b2e305c4e1c1

Directory Of Scam Sites

Cocaine - Heroin
Ketamine - LSD
MDMA - Crack

dread frontpage all dread

1 billion Chinese residents' data've been allegedly leaked & sold on CCP Founding Day
by /u/Oran - in /d/CafeDread

Social network in China has already censored all news & posts on this massive leak, so netizens have begun posting that there was 23.88TB database leak happened in other countries...

cracking Forums What's new

Premium Accounts

Free premium accounts can be found here.
We supply accounts to file hosts sites and much more.

http://breached65
Police-database

Quote:

Finding Email Password Dumps

Install and configure h8mail

Combining TheHarvester and Crosslinked tools, you can see if an organizations email address have been compromised.

```
apt install python3-pip
Pip3 install h8mail
cd /home/kali/.local/bin
```

Acquire and install API keys, this provides you the option to use premium services.

```
Python3 h8mail -g
```

```
$> view /home/kali/.local/bin/h8mail_config.ini (enter your api here after hibp)
```

```
Python3 h8mail -h
```

```
Python3 h8mail -t <target email address>
```

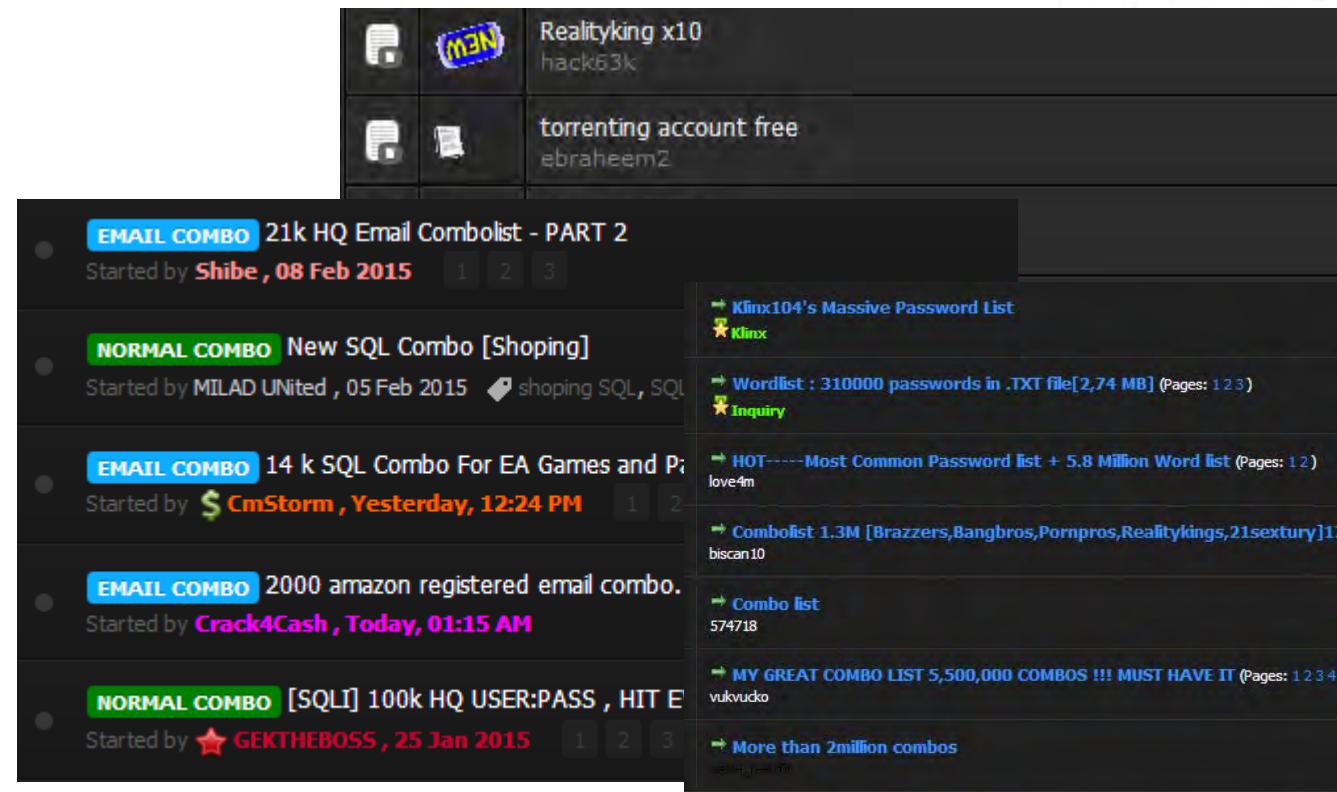
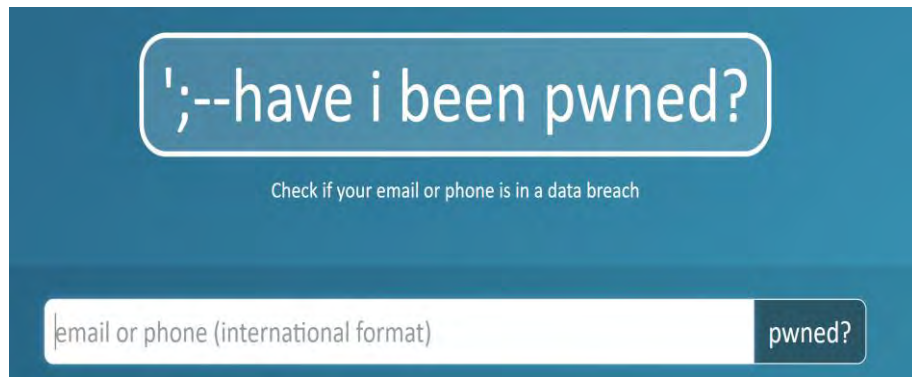
```
Python3 h8mail -t victim@email.com -c /home/kali/.local/bin/h8mail_config.ini -o savefile
```



Finding breach and stealer data

HIBP: <https://haveibeenpwned.com/>

Keeper: <https://www.keepersecurity.com/free-data-breach-scan.html>

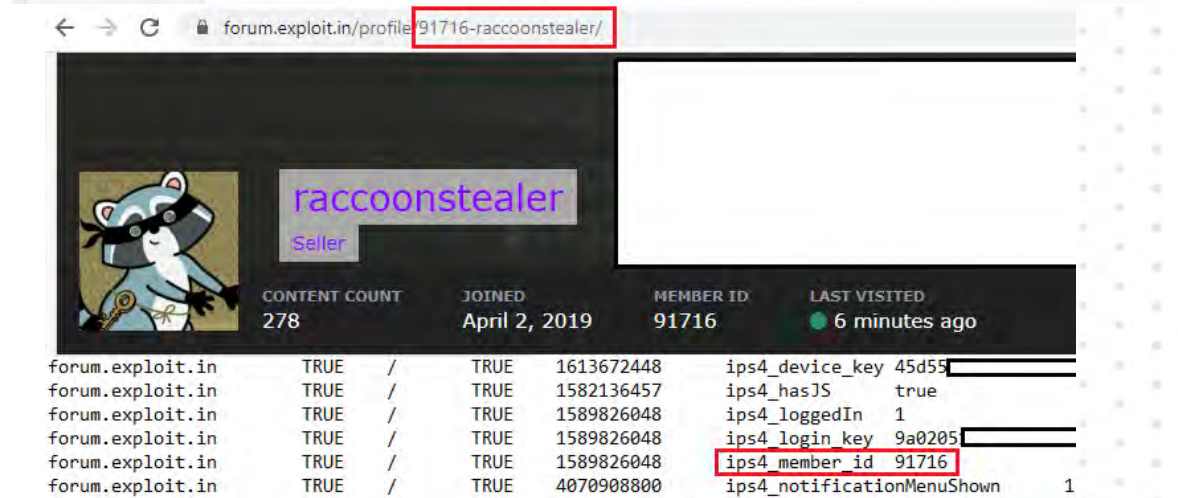
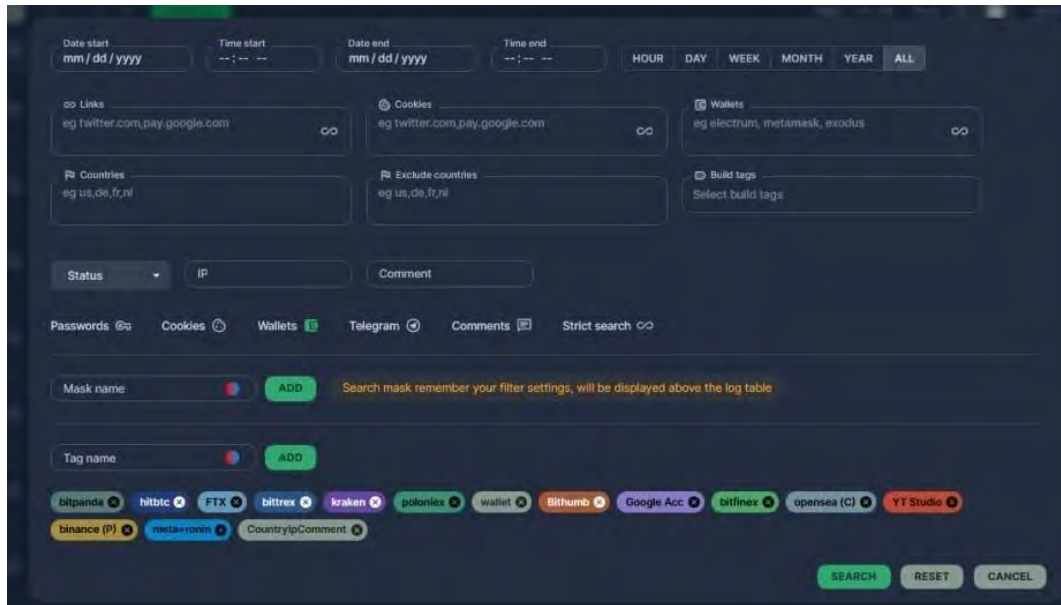


<https://scatteredsecrets.com/>

<https://cybernews.com/personal-data-leak-check/>

Finding data – Info/Cloud Stealers

Raccoon Stealer:



<https://www.google.com/search?hl=en&q=%22premium%20accounts%22>

Mobile dark(net) markets



bright data
Mobile proxies
Enjoy the fastest and largest real-peer 3G/4G IPs in Bright Data's advanced mobile network.

[Start now](#) [Pricing](#)



<https://telegramindex.com/telegram/channels/>
<https://tgstat.ru/en>



Performing Dark Web Reconnaissance

Hunchly Daily Dark Web Reports are probably a good place to start. There's two ways of going about this. Hunchly is a discovery tool it explicitly states they do not analyze the hidden services for content. The links you receive could lead to drug markets, child pornography, malware, or other sensitive content be careful this gets stored on your system. Hunchly is not responsible for the dissemination of such content; use at your own discretion.

Dark Search a reliable dark web search engine with the ability to use advanced search operators. You can view this search engine on any web browser but you will only be able to follow the links found in its index by using Tor or similar. While their search operators are not as robust as Google Dorks, you *can* achieve quite specific results with the ones they offer. I really like the boost operator (^) that allows you to emphasize a term in your search query.

And Some websites and tools:

Reddit | Pastebin | Maltego | Hunch.ly | Selenium | Pandas | Discord | Twitter

Darknetlive

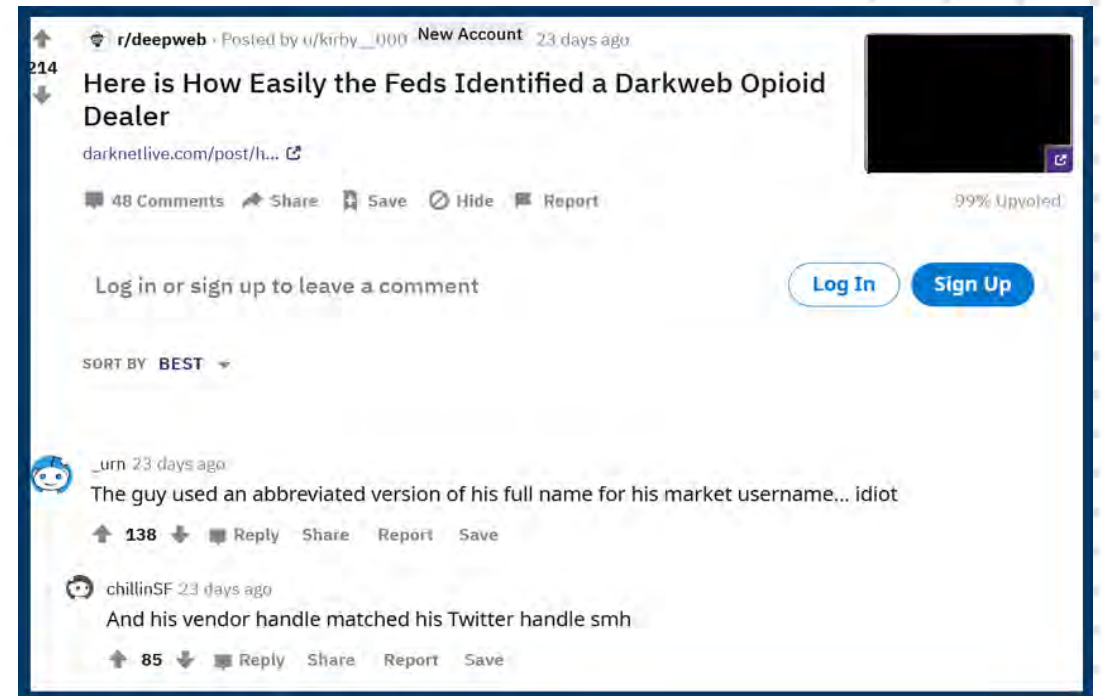
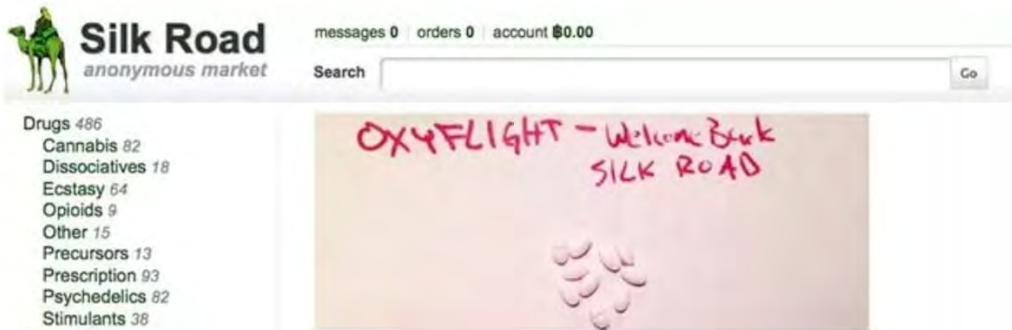
Home Arrests Markets Forums Onions Shops

[Home](#) / [Posts](#) / [Feds Traced Bitcoin Transactions to a Drug Dealer's Apartment](#)

Feds Traced Bitcoin Transactions to a Drug Dealer's Apartment

Federal investigators identified a darkweb opioid dealer by linking Bitcoin transactions to the dealer's home I.P. address.

Daren James Reid, 35, of Fort Lauderdale, used darkweb markets to distribute oxycodone, according to [a recent plea agreement](#). Using the monikers "Oxyflight" and "Imperial Royalty," Reid sold over 12,000 oxycodone pills on Silk Road, WallStreet Market, Apollon, Dream, and other markets. He also admitted selling between 3,000 and 10,000 kilograms of marijuana. The sales yielded more than \$500,000 in gross profit, the government announced. During a raid of a storage facility used by Reid, police found over one kilogram of oxycodone, morphine, and other pills.



Darkweb Search Engine sites:

Onion Land - <http://3bbad7fauom4d6sgppalyqddsqb5u5p56b5k5uk2zxsy3d6ey2jobad.onion/>

Tourch - <http://xmh57jrknzkhv6y3ls3ubitzfqnrwxhopf5aygthi7d6rplyvk3noyd.onion/cgi-bin/omega/omega>

Ahmia - Ahmia.fi

Ahmia Tor - <http://juhanurmihxlp77nkq76byazcldy2hlmovfu2epvl5ankdibsot4csyd.onion/>

TOR 66 - <http://tor66sewebgixwhcqfnp5inzp5x5uohhdy3kvtnyfxc2e5mxiuh34iid.onion/fresh>

Phobos - <http://phobosxilamwgcg75xt22id7aywkzol6q6rfl2flipcqoc4e4ahima5id.onion/>

- **Markets, Forums & Chat Groups:**

- Markets:

- Stolen Data
- Malware
- Database Dumps
- Stolen Credentials

- Forums:

- Exchange ideas along with sales to each other
- admin arbitration
- Darkweb User/Community feedback is key

- Chat Groups

- Telegram, ICQ, QQ, discord and others
- Rapidly changing and hard to keep up with

- **Establishing a Presence**

- Dedicate a lot of time

- Active Forum and chat participation
- leaving for extended times blows your cover

- Learn the lingo, social engineering, friend others

- **Infrastructure:**

- VPN Service and Tor are Key used to ban certain countries
- Tor Markets and Forums

- Blockchain DNS

- Russian Darkweb likes .SU tld

- **Osint**

- Do your homework

- Learn about the platforms, and the rules
- Learn who the common/popular users are

- limit your comments on the forums

- Keep it positive at all times

- Do not post real opinions

Crime Search Engines

darkfailenbsdla5mal2mxn2uz66od5vtzd5qozslagrffzachha3f3id.onion

dark.fail: Is a .onion site online?

Updated Sun, 23 Oct 2022 18:38:13 UTC
[Mastodon](#) | [Twitter](#)

You are on the clearnet. It is not recommended to view our site here. Domain names are not as secure as Tor hidden services. Install Tor Browser and visit us at our .onion instead:

darkfailenbsdla5mal2mxn2uz66od5vtzd5qozslagrffzachha3f3id.onion [Verify](#)

NEW: Verify signatures with Dark.fail's [new PGP Tool](#). Don't get phished. Always PGP verify .onion and Bitcoin addresses before interacting with them.

Tor is the uncensored internet. Install [Tor Browser](#) to explore it. Set darkfailenbsdla5mal2mxn2uz66od5vtzd5qozslagrffzachha3f3id.onion as your home page to save time. Links are PGP verified and unclickable for your safety. dark.fail's [philosophy](#) and [finances](#)

This resource is intended for researchers only. We do not vouch for any sites.

Darknet Live

- <http://darkkzx4avcsuofgfez5zq75cqc4mprjvfgywo45dfcaxrwgg6qrlfid.onion>

Dread

Offline:

<http://dread2ytot03vpt0d7n10113v>
< [] >

Recon

Offline:

<http://recon232tth4nb7u7dhbn9s4>
< [] >

403 DDOS filter killed your path. (You probably sent too many requests at once). Not calling you a bot, bot, but grab a new identity and try again.



PhoneInfoga

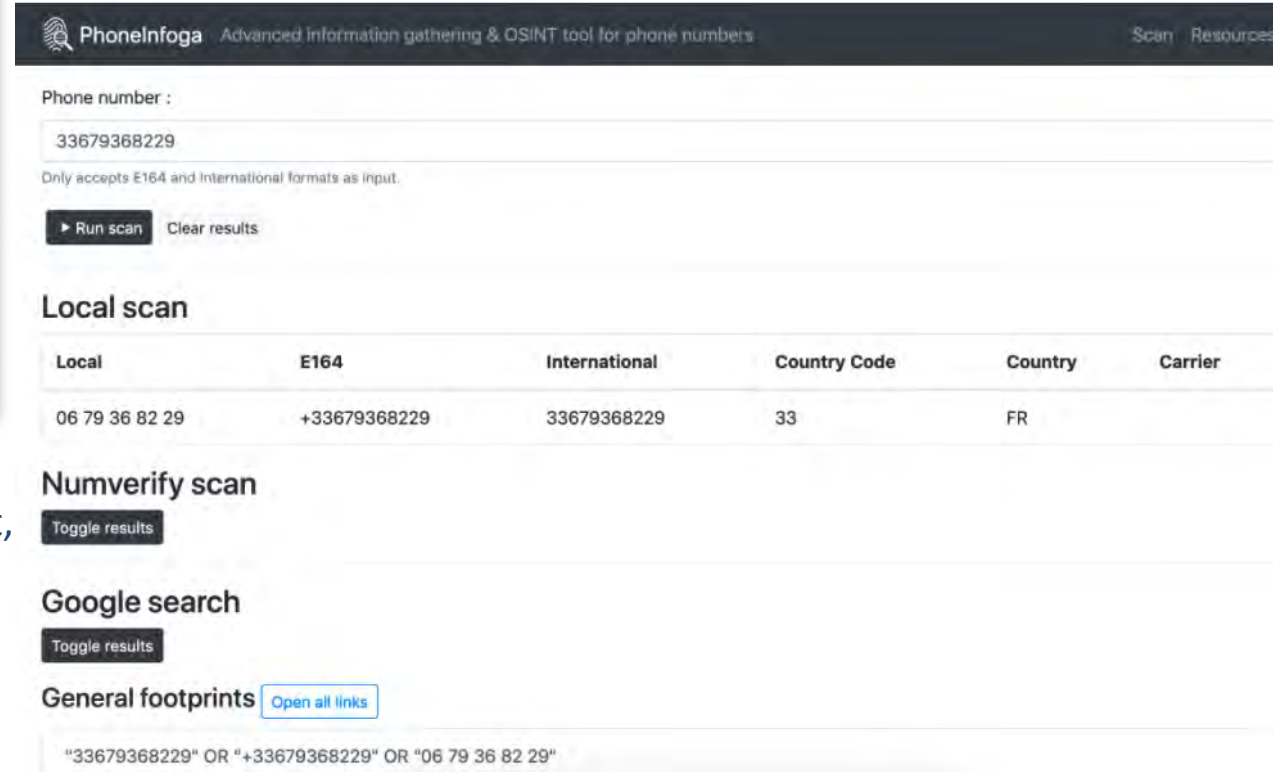
Build passing go report A+ maintainability A coverage 95% release v2.4.2

Advanced information gathering & OSINT framework for phone numbers

[Documentation](#) • [API documentation](#) • [Demo instance](#) • [Related blog post](#)

A phone number may not seem like much information to give out, an OSINT researcher can quickly discover information that ties a phone number to a variety of other clues.

<https://github.com/sundowndev/phoneinfoga>



PhoneInfoga Advanced information gathering & OSINT tool for phone numbers Scan Resources

Phone number :
33679368229

Only accepts E164 and International formats as input.

▶ Run scan Clear results

Local scan

| Local | E164 | International | Country Code | Country | Carrier |
|----------------|--------------|---------------|--------------|---------|---------|
| 06 79 36 82 29 | +33679368229 | 33679368229 | 33 | FR | |

Numverify scan

Toggle results

Google search

Toggle results

General footprints

Open all links

"33679368229" OR "+33679368229" OR "06 79 36 82 29"

OSINT Tools & Techniques for the Dark Web

As OSINT investigators, collectors, and analysts, all must be familiar with the dark web and be able to navigate it with efficiency, as well as steer clear of dangers. We also have to be able to extract information from it, about a targeted, in an efficient manner. These tools can be used to get started and get you comfortable inspecting the dark web.

Hunchly - <https://www.hunch.ly/darkweb-osint/>

DarkSearch - <https://darksearch.io/>

TorBot - <https://github.com/DedSecInside/TorBot>

Fresh Onions - <https://github.com/dirtyfilthy/freshonions-torscraper>

TorCrawl - <https://github.com/MikeMeliz/TorCrawl.py>

Onion.Live - <https://onion.live/>

IACA Dark Web Invest - <https://iaca-darkweb-tools.com/>

Onion Nmap - <https://github.com/milesrichardson/docker-onion-nmap>

Onion Scan - <https://github.com/s-rah/onionscan>

OniOff - <https://github.com/k4m4/onioff>

Onion Ingestor - <https://github.com/danieleperera/OnionIngestor>

Katana <https://github.com/adnane-X-tebbaa/Katana>

As OSINT investigators, collectors, and analysts, all must be familiar with the dark web and be able to navigate it with efficiency. We also have to be able to extract information from it in a targeted, efficient matter. These tools can be used to get started, get you comfortable inspecting traffic and data on the dark web.

H-Indexer <http://jncyepk6zbnosf4p.onion/onions.html>

Provides a list of the onions it has indexed including language, title, URL & last contacted in text format

TOR66 <http://tor66sewebgixwhcqfnp5inzp5x5uohhdy3kvtnyfxc2e5mxiuh34iid.onion/fresh>

Rolling set of identified .onions. This includes the time it was seen, the description & the language identified

Hunch.ly: a web capture tool and case management tool designed specifically for online investigations.

Investigating people on the dark web usually comes down to attribution between the surface & dark web through information slippage. This is where the same attributable markers, e.g. usernames, ID's, PGP keys, cryptocurrency addresses, email addresses, social media, are used by actors on both the surface & dark web.

Hunchly & Maltego



1st Select

2nd - Select

Import Wizard

STEPS

- Select File
- Selection
- Import

SELECT FILE: Choose the Maltego archive file (containing configuration items) to import from your file system.

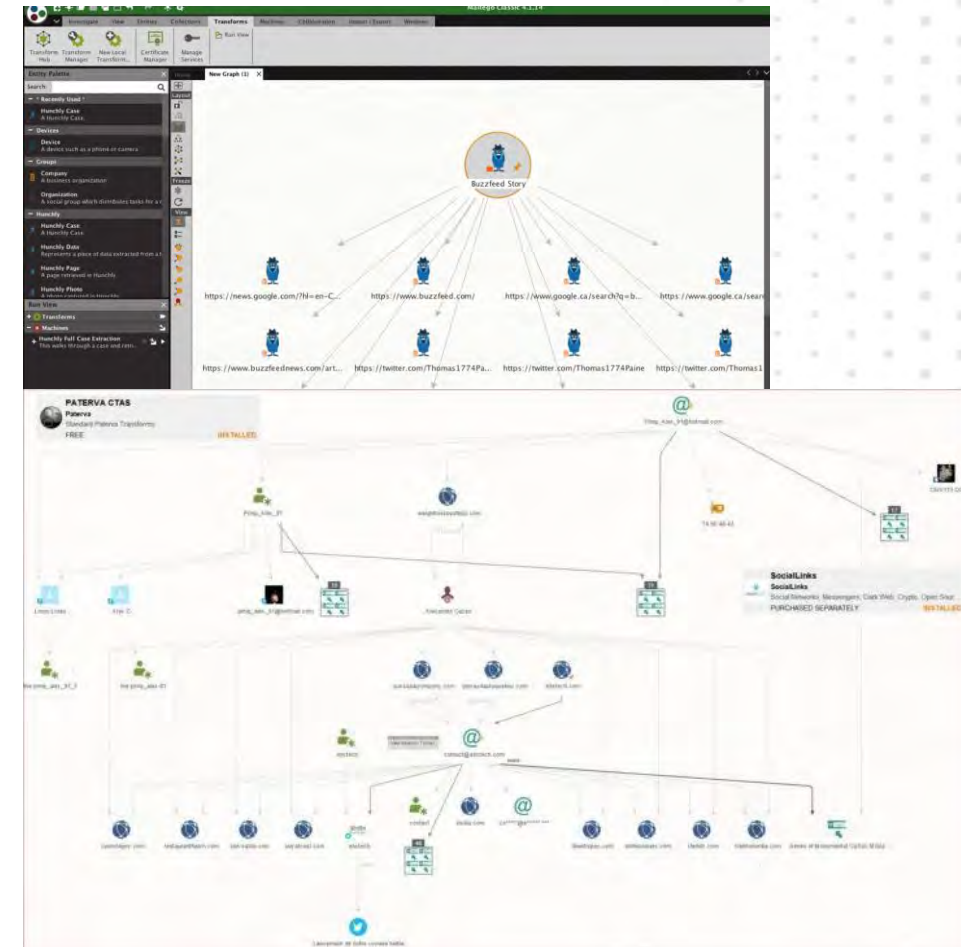
Look In: Documents/HunchlyMarketing/maltego

python
hunchlyconfiguration.mtz

SELECTION: Select the configuration items you which to import from the Maltego archive file.

| Name | Description |
|--|---------------------------|
| <input checked="" type="checkbox"/> Entities | 1 Categories (6 Entities) |
| <input checked="" type="checkbox"/> Local Transforms | 8 Transforms |
| <input checked="" type="checkbox"/> Transform Sets | 1 Transform Sets |
| <input checked="" type="checkbox"/> Machines | 1 Machines |
| <input checked="" type="checkbox"/> Icons | 1 Categories |

< Back Next > Cancel



dnstats

DARKNET MARKETS VENDOR SHOPS CARD SHOPS

World Market

Visit Site

WORLD MARKET IS UP

worldmpls3c2idbjzdmbs4wt4dfqfjavptjos4se444uk5v23q2wbyd.onion

World Market

In order to check you are a human, please write down the captcha you are seeing.

DDOS PROTECTION



What do you see in the Captcha?

Visit World Market

WorldMarket

Home Messages 32 Orders Become A Vendor Deposit/Withdraw Profile Forum Support Bible

1 BTC = USD 44138

Logged in as: c...

View Profile Logout

Settings My Autoshop

1 Unread Notifications

Home

Profile



Joined: 2 years
Trust level: Buyer Level 1
Total orders: 0.01029 BTC
Total orders: 2.91451 XMR
Disputes won / lost: 0 / 0

Warning

World Market is not going anywhere, we are always here to help our community. In case of any issue, contact us immediately.

Danger

Don't get phished, always verify the PGP signatures of the deposit addresses!

Warning

We highly recommend that you disable Javascript when viewing the marketplace for better security!

Shop By Categories

- Drugs 36353
- Fraud 8776
- Digital goods 4466
- Counterfeit Items 725
- Services 1807

Welcome, c...

Quick Search

Search

Show Advanced Search

World Market

You have been placed in a queue, awaiting forwarding to the platform.

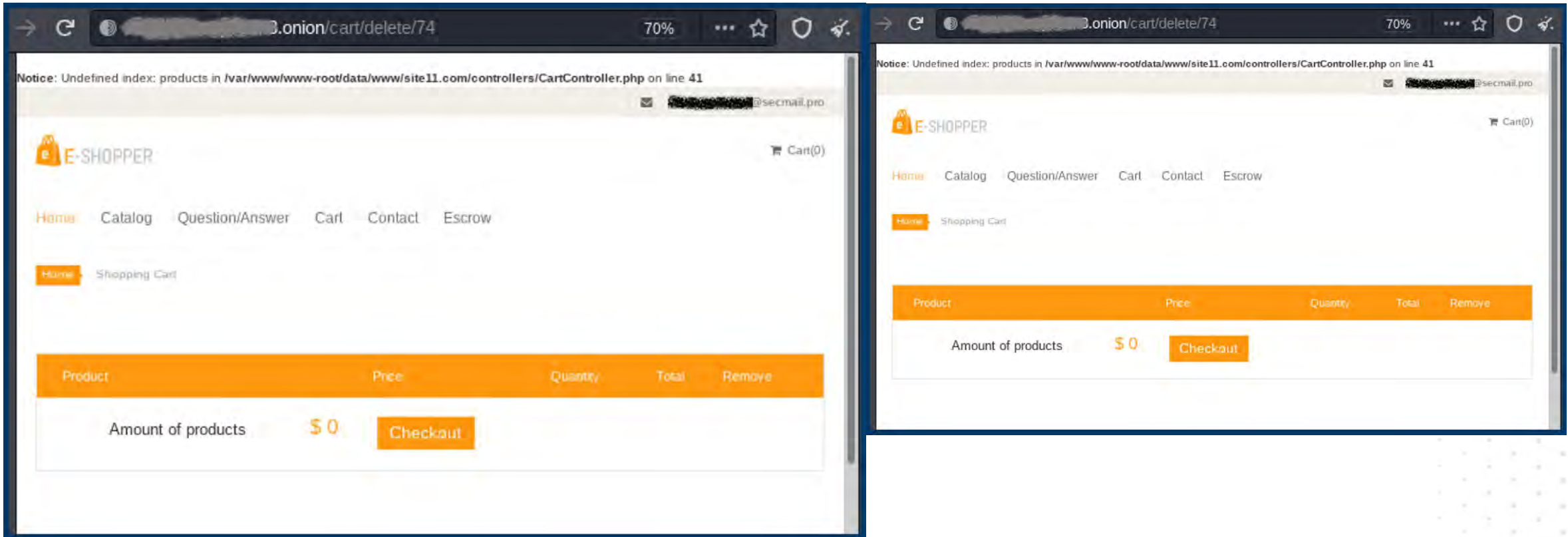


Your estimated wait time is <2 minutes

Please do not refresh the page, you will be automatically redirected.

WebApp bugs in the Dark

OSINT Gathered from a Bug Hunters perspective



Index of /controllers

| Name | Last modified | Size | Description |
|---|------------------|------|-------------|
| Parent Directory | - | - | - |
| AdminCategoryController.php | 2019-05-23 13:25 | 1.9K | |
| AdminController.php | 2019-05-23 13:25 | 214 | |
| AdminCountryController.php | 2019-05-23 13:25 | 1.2K | |
| AdminDeliveryController.php | 2019-05-23 13:25 | 1.2K | |
| AdminOrderController.php | 2019-05-23 13:25 | 1.6K | |
| AdminProductController.php | 2019-05-23 13:25 | 4.2K | |
| AdminPurseController.php | 2019-05-23 13:25 | 1.2K | |
| AdminStateController.php | 2019-05-23 13:25 | 1.1K | |
| CartController.php | 2019-05-23 13:25 | 4.7K | |
| CatalogController.php | 2019-05-23 13:25 | 1.1K | |
| ProductController.php | 2019-05-23 13:25 | 399 | |
| SiteController.php | 2019-05-23 13:25 | 1.6K | |
| UserController.php | 2019-05-23 13:25 | 1.0K | |

SHOPPER

Cart(3)

[Catalog](#) [Question/Answer](#) [Cart](#) [Contact](#) [Escrow](#)

CATEGORY

CATALOG

WABIS

OS CANNABIS

MAINE

FLORIDA

Warning: Invalid argument supplied for foreach() in /var/www/www-root/data/www/site11.com/views/catalog/catalog.php on line 10

nginx/1.16.0

Warning: call_user_func_array() expects parameter 1 to be a valid callback, class "SiteController" does not have a method "actionIndexcsite" in /var/www/www-root/data/www/site11.com/components/Router.php on line 45

Bugs in Popular webservers, carts, webapps.

10 – Remote Code Execution

Remote Code Execution occurs when an attacker is able to execute code on a target system in a way that is unintended. It's hard to believe how common Remote Code Execution (RCE) vulnerabilities have been so far this year.

There are many different ways to achieve RCE, but some ideas are:

- Abusing file upload functionality to upload a webshell
- Deserialization bugs
- Exploiting known CVEs
- Command injection

1 – Sensitive data exposure

2 – Cross-Site Scripting

3 – SubDomain Takeover

4 – Broken Access Control – IDOR

5 – Privilege Escalation

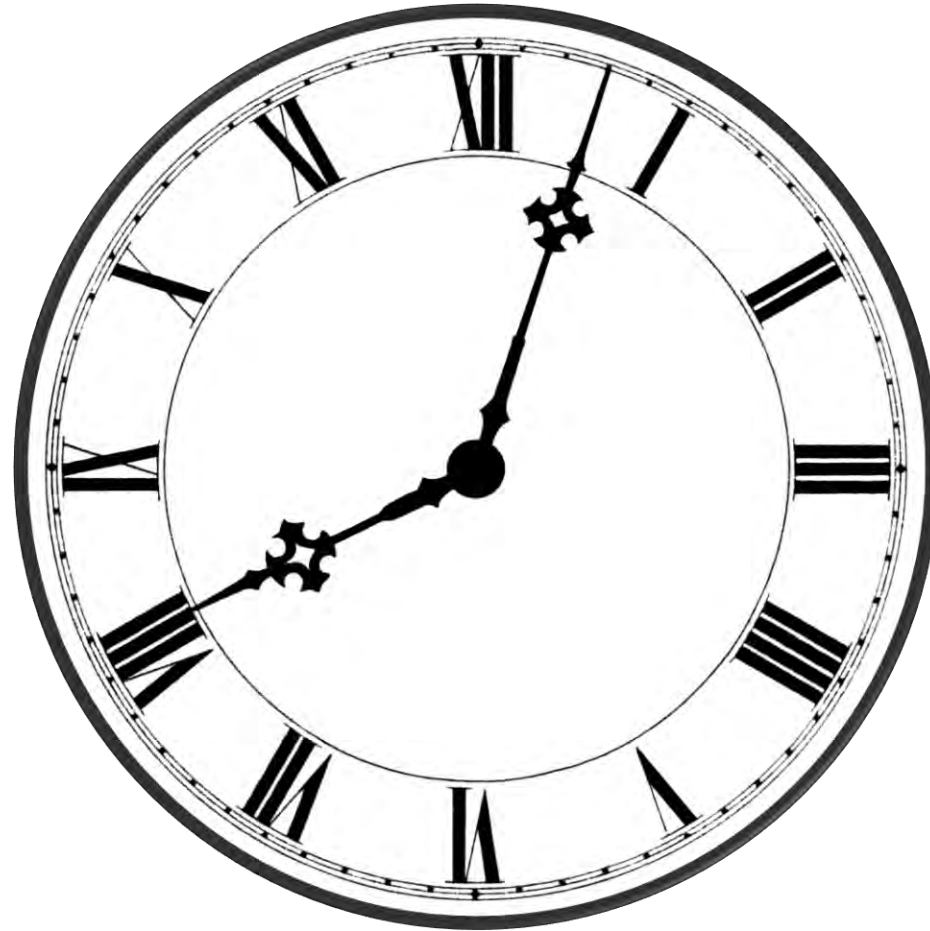
6 – Sensitive Info Passed to http

7 - Authentication bypass

8 – Cross Site Request Forgery (CSRF)

9 – Open Redirect

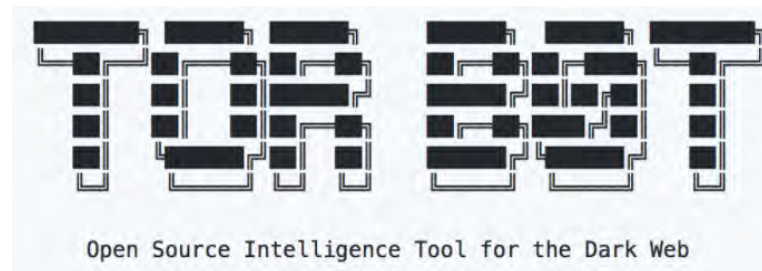
Break – 5 min.



TorBot Darkweb Crawlers

Docker version of Trandosan: <https://github.com/trandoshan-io/k8s>

It has been moved over to creekorful – and is Bathyscaphe dark web crawler
<https://github.com/darkspot-org/bathyscaphe>



trandoshan-io/
crawler



Go process used to crawl websites

2 Contributors 0 Issues 149 Stars 19 Forks

TorBot: <https://github.com/DedSecInside/TorBot>

GoTor: <https://github.com/KingAkeem/gotor>

Dark Web investigative tools

DarkOwl Vision Professional Tools

Enter search here

DARKINT Search Lexicon

| Markets | Offerings |
|---|--|
| Actors | |
| Markets | |
| Vendors | |
| Forums | |
| Actopis | Fraud, Digital goods/services |
| AeroFlat | Drugs |
| Apollon | Drugs, Fraud, Miscellaneous |
| Berkusori | Drugs, Fraud, Miscellaneous |
| Carriable Growers and Merchants Cooperative | Drugs |
| Carvazon | Drugs |
| Dream Market | Drugs, Digital goods/services |
| DRUGSTORE | Drugs |
| DutchDrugs's Psychiadelicum | Drugs |
| Empire Market | Drugs, Digital goods/services, Miscellaneous |
| FastFooduk | Drugs |

Intelligence Dashboard

Latest intelligence by target country

Oct. 8, 2018 12:31:57

- Intelligence Dashboard
- Actors
- Reports & Feeds
- Indicators
- Tailored Intelligence
- Submit Malware
- Subscriptions

DarkTracer (Pro)

ip:80.85.158.81 Analysis

DarkTracer (Pro) ✓

NETWORK INFO

- Tor Domain: http://25wcyz.../server-status
- Tor URL: http://1s6xck.../server-status
- http://gg7cb4.../server-status
- IP: http://uuecxj.../server-status
- Domain (Nisookus): http://7uvipl.../server-status
- Server Status: http://pharma.../server-status
- Custom Info: http://7uvijs.../server-status
- External Search Info: http://cocain.../server-status
- Google Search: http://treaty4.../server-status

INTELLIGENCE INFO

CUSTOM INFO

EXTERNAL SEARCH INFO

Google Search

80.85.158.81

Crystal meth ice shards

Configuration

- Prevention Policies
- Sensor Update Policies
- Custom IOA Rule Groups
- USB Device Policies
- Response Policies
- Response Scripts & Files
- File Exclusions
- Prevention Hashes
- Containment Policy
- Upload Quarantined Files
- Mobile Policies
- General Settings

Prevented malware by host (last 7 d...)

| TACTIC & TECHNIQUE | DETECT TIME | HOST |
|----------------------------------|------------------------|-----------------|
| High Falcon Intel via Inte... | Jan. 13, 2020 09:21... | SE-VAL-WIN10-DT |
| Critical Exfiltration via Dat... | Jan. 13, 2020 09:21... | SE-VAL-WIN10-DT |
| Low Falcon Overwatch v... | Jan. 13, 2020 08:58... | SE-CVI-WIN10-DT |
| Medium Execution via Powe... | Jan. 13, 2020 08:55... | SE-CVI-WIN10-DT |

Detections by Tactic (Last 30 days)

Latest Intelligence

- Jan. 13, 2020 09:46:45 CSIR-19010 DPRK Wiper Operations: Motivations and Objectives
- Jan. 10, 2020 19:11:32 CSA-200050 Ongoing PIRATE PANDA Operations Using Killswitch Domains, Co...
- Jan. 10, 2020 18:49:08

Host your own Tor Server?

Because Tor is dynamic and intentionally re-routes traffic in unpredictable ways, an onion address makes both the information provider (you) and the person accessing the information (your traffic) difficult to trace by one another, by intermediate network hosts, or by an outsider. Generally, an onion address is unattractive, with 16-character names like 8zd335ae47dp89pd.onion. Not memorable, and difficult to identify when spoofed, but a few projects that culminated with Shallot (forked as eschalot) provides "vanity" onion addresses to solve those issues.

Creating a vanity onion URL on your own is possible but computationally expensive. Getting the exact 16 characters you want could take a single computer billions of years to achieve, an 8 character URL is about 25 days, beyond that it takes years.

Create your own Darkweb Vanity URL - <https://github.com/cathugger/mkp224o>

Exercise 8

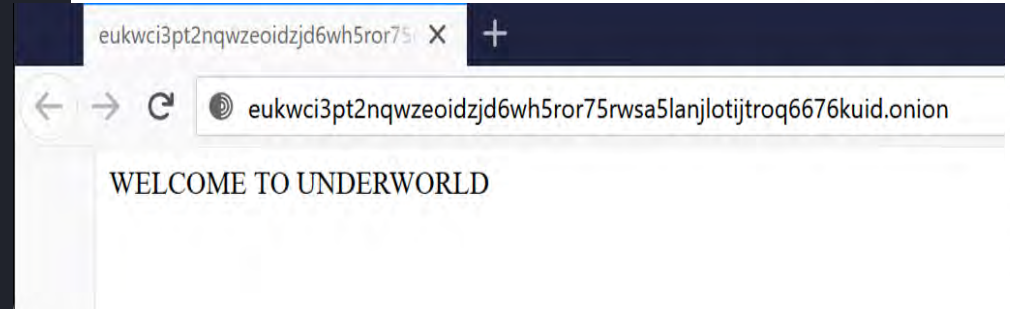


LET'S BUILD A TOR SERVER

```
##### This section is just for location-hidden services ###  
  
## Once you have configured a hidden service, you can look at the  
## contents of the file ".../hidden_service/hostname" for the address  
## to tell people.  
##  
## HiddenServicePort x y:z says to redirect requests on port x to the  
## address y:z.  
  
#HiddenServiceDir /var/lib/tor/hidden_service/  
#HiddenServicePort 80 127.0.0.1:80
```

```
HiddenServiceDir /var/lib/tor/hidden_service/  
HiddenServicePort 80 127.0.0.1:8080
```

```
(root@THX)-[~]  
# cd /var/lib/tor/hidden_service  
  
(root@THX)-[/var/lib/tor/hidden_service]  
# ls  
authorized_clients  hostname  hs_ed25519_public_key  hs_ed25519_secret_key  
  
(root@THX)-[/var/lib/tor/hidden_service]  
# cat hostname  
eukwci3pt2nqwzeoidzjd6wh5ror75rsa5lanjlotijtroq6676kuid.onion  
  
(root@THX)-[/var/lib/tor/hidden_service]  
#
```











```
HiddenServiceDir /var/lib/tor/hidden_service/http  
HiddenServicePort 80 127.0.0.1:80  
HiddenServiceDir /var/lib/tor/hidden_service/ssh  
HiddenServicePort 22 127.0.0.1:22
```










Outsource your Tor Server

Tor Hosting Providers

Looking for **Tor hosting providers – DMCA ignored hosting & bullet proof hosting** to host your **darknet** websites? Here is the list of TOP **deep web hosting service providers** and their features with Cryptocurrencies Payment details. Some of the **hosting services** are 100% anonymous as it doesn't require any documents or identify proofs and are offshore in most instances. They also accept **Bitcoin** and other **cryptocurrencies**.

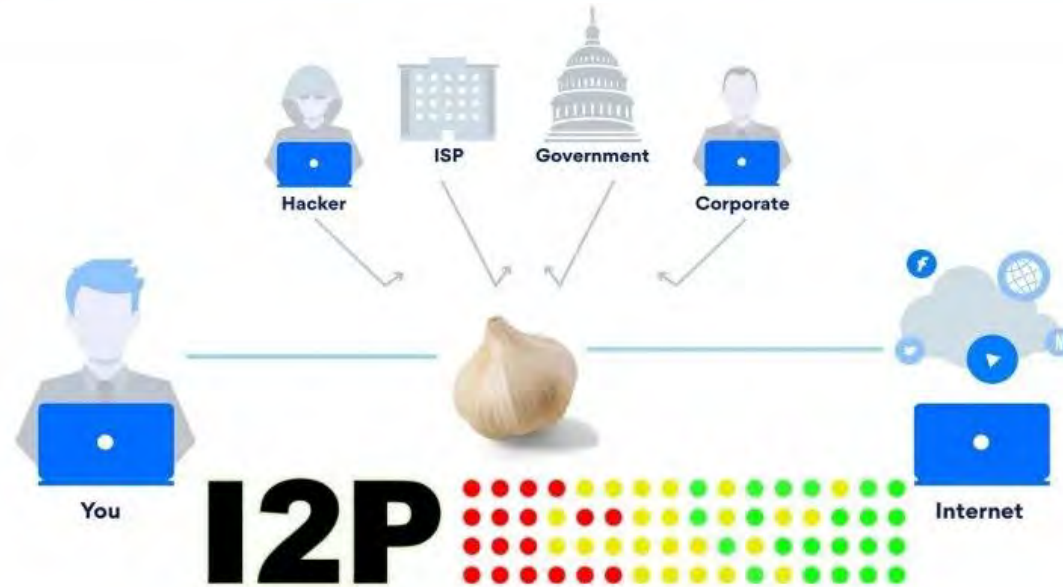
| Sl. No | Company - ISP | Country | Bridges | Relay | Exit | Features | Crypto support | Website |
|--------|---|----------|-------------------------------------|-------------------------------------|-------------------------------------|---|---|----------------------------|
| 1 |  | Dominica | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | KVM Dedicated resources SSD or NVMe drives only Anti-DDoS Protection Full Disk Encryption Premium support |  +4 | Visit site |
| 2 |  | Nevis | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | 100 % Domain privacy Anycasted DNS Virtual Private Server OK Support Root Access |  +3 | Visit site |
| 3 |  | Bulgaria | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | SSD Storage 1 TB/s DDos Protection offshore location Powerful CPU Root access |  | Visit site |
| 4 |  | sweden | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Cold War Bunker Powerful IP services Shell protection Nuclear Bunker Hosted Wikileaks * |  via Support | Visit site |

Payment Method

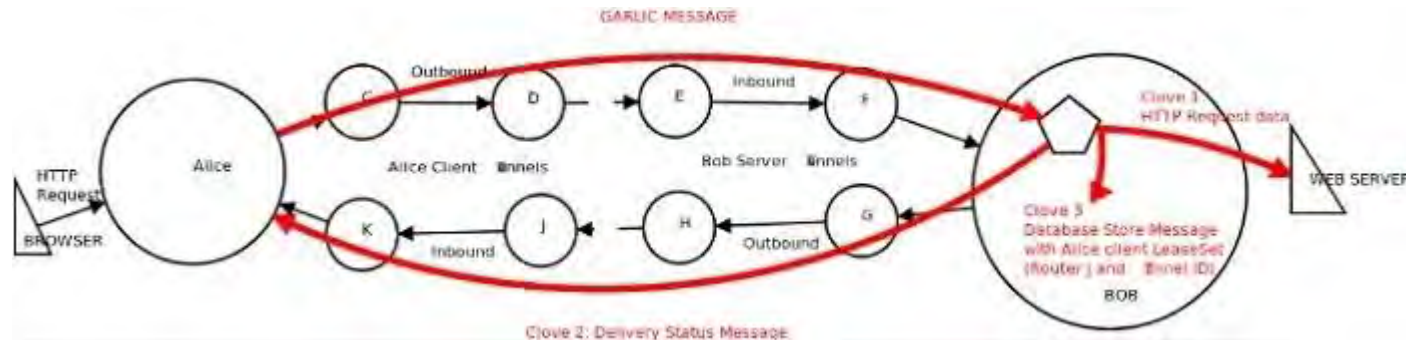
-  Bitcoin
-  Bitcoin Cash
-  Dash
-  Ethereum
-  Litecoin
-  Monero
- PerfectMoney (+ 3.20%)
-  Zcash

[Checkout](#)

Invisible Internet Project (I2P)

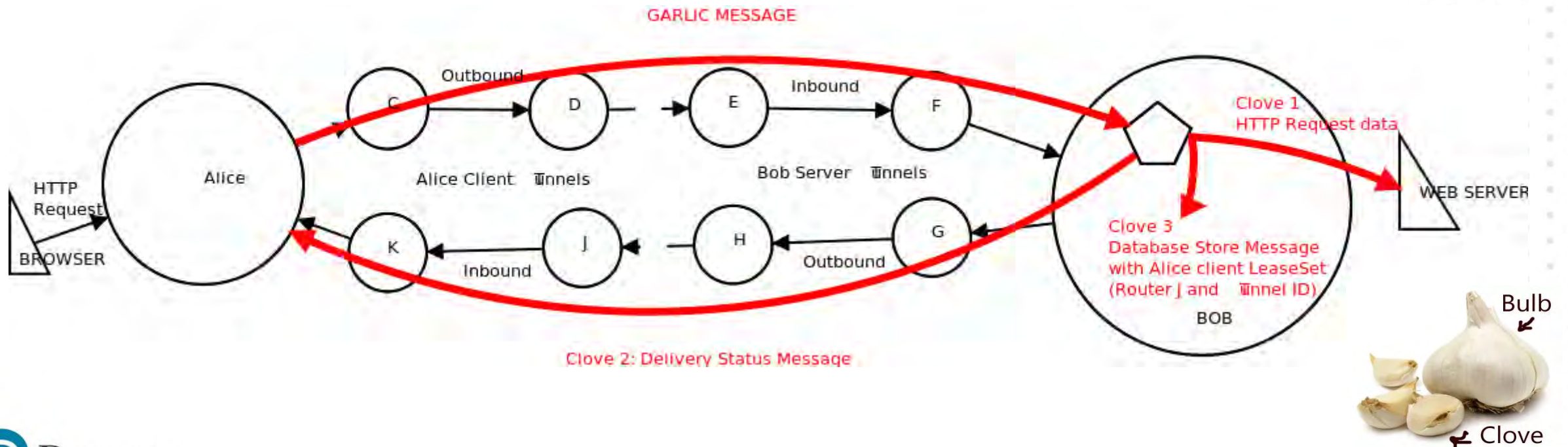


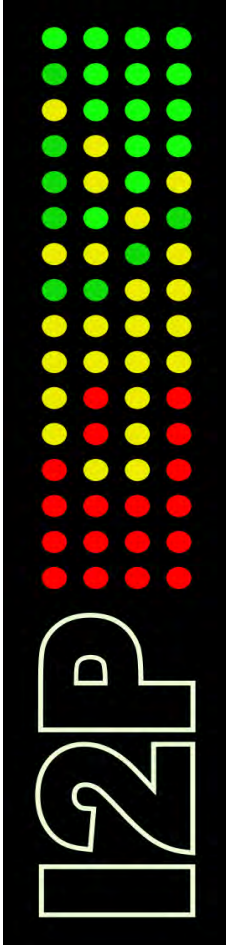
Garlic routing is an improved browsing technology that leverages multiple encryption routes to anonymize your Internet traffic from corporations, governments, hackers and ISPs. In this regard, it has a similar purpose as onion routing, which uses Tor-encrypted networks to deliver anonymity.



The biggest advantage of this “garlic” technique is that it is peer-to-peer friendly because the “delivery status message” uses a separate route compared to the “garlic message.” Therefore, by using a different reply block, garlic routing turns the very concept of world wide web on its head. The idea is to ensure greater protection against detection of client activity, even when an attacker is participating in the tunnel.

The Invisible Internet Project (I2P) has contributed in a major way to garlic routing. While the anonymous browsing project seems to be in a beta phase, you can use it right now without any problems.





127.0.0.1:7657/home

I2P Router Console - N...

I2P Router Console

Feb 25, 2021 Congratulations On Getting I2P Installed!

Welcome to I2P! Please have patience as I2P boots up and finds peers.

While you are waiting, please [adjust your bandwidth settings](#) on the [configuration page](#).

Also you can setup your browser to use the I2P proxy to reach eepsites. Just enter 127.0.0.1 (or localhost) port 4444 as a http proxy into your browser settings. Do not use SOCKS for this. More information can be found on the [I2P browser proxy setup page](#).

Once you have a "shared clients" destination listed on the left, please [check out our FAQ](#).

Point your IRC client to `localhost:6668` and say hi to us on `#i2p`.

Version: 0.9.49-0-1ubuntu1
Uptime: 4 min

| Bandwidth In/out | |
|------------------|------------------|
| 3 Sec: | 0.00 / 0.02 KBps |
| Total: | 0.27 / 1.07 KBps |
| Used: | 94.1 KB / 254 KB |

Network: Firewallled

Reseed successful, fetched 154 router infos

Local Tunnels

- shared clients

Applications

- Address Book
- Email
- Hidden Services Manager
- Torrents
- Web Server

I2P Community Sites













- Dev Forum
- Git Project Hosting
- I2P FAQ
- I2P Forum
- I2P Pastebin
- MuWire
- Planet I2P
- Project Website
- The Tin Hat

Configuration And Help

- Settings
- Home
- Help
- Logout
- Refresh



- **Katana** - <https://github.com/adnane-X-tebbaa/Katana>
- **OnionSearch** - <https://github.com/megadose/OnionSearch>
- **Darkdump** - <https://github.com/josh0xA/darkdump>
- **Ahmia Search Engine** - ahmia.fi, <https://github.com/ahmia/ahmia-site>
- **DarkSearch** - <https://darksearch.io/>, <https://github.com/thehappydinoa/DarkSearch>
- **Tor66 Fresh Onions** - <http://tor66sewebgixwhcqfnp5inzp5x5uohhdy3kvtnyfxc2e5mxiuh34iid.onion/fresh>
- **RECON** - <http://recon222ttn4ob7ujdhbn3s4gjre7netvzybuybq2bcqwltkiqinhad.onion/>
- **Onion Web** - <http://onionwsoiu53xre32jwve7euacadvhprq2jyfttb55hrbo3execodad.onion/>
- **Deep Markets** - <https://deepwebmarketsreview.com/>
- **Hidden Index** - <https://hiddenindex.org/>

| | | | |
|--|--|---|---|
|  AlphaBay ★★★★★ Multisig |  Archetyp Market ★★★★★ |  ASAP Market ★★★★★ |  Bohemia ★★★★★ |
|  CannaHome ★★★★★ Multisig |  Cypher Market ★★★★★ |  Dark0de Reborn ★★★★★ Multisig |  DarkFox Market ★★★★★ Multisig |
|  Incognito Market ★★★★★ |  Tor2door Market ★★★★★ Multisig |  Versus ★★★★★ Multisig Only |  World Market ★★★★★ |



More at DarkWeb.sh

Twitter: @Cedoxx

Discord:
<https://darkweb.sh/discord>