The Deep Web, the Darknet, and Bitcoin

Elisa Cooper & Akino Chikada
MarkMonitor
Agenda

- Deep Web vs Darknet
- Tor
- Underground Marketplaces
- Role of Bitcoin
- Strategies for Mitigating Abuse
- Q&A Session
Understanding the Internet Landscape

Surface Web
Searchable with standard search engines

Deep Web
Un-indexed websites

Dark Web / DarkNet
Dark Web: web content that exists on the DarkNet
DarkNet: Network that can only be accessed with specific software, configurations, or authorization

The Deep Web is hundreds of times larger than the ‘Surface Web’
What's in the Deep Web?

- 96% of the content exists in the deep web
  - 7500+ TB of content

- Types of content that is in the deep web:
  - Dynamic content
  - Unlinked content
  - Private Web
  - Contextual Web
  - Limited access content
  - Scripted content
  - Non-HTML/text content
  - Software
  - Web archives
  - Un-indexed websites
  - P2P networks
Deep Web Content

Not Everything in the Deep Web is Seedy

- Forms
- Login / Paywall
  - Corporate Intranet
  - Social Media Sites
- No URL
Deep Web Content of Concern

- Any un-indexed web page
  - Selling counterfeit or grey market goods
  - Collecting user credentials
  - Disseminating malware
  - Engaged in false association
  - Conducting consumer scam

- P2P sites where piracy taking place

- Marketplaces where counterfeit, grey market or unauthorized goods are sold

- Social media where impersonation is occurring
How Are Consumers Directed to the Deep Web?

- Websites
- Social Media
- Email
- Paid Search
- Mobile Apps
So What Is the Darknet?

- Within the Darknet both web surfers and website publishers are entirely anonymous
- Anonymity is usually achieved using Tor
- There are a number of marketplaces (the online black market)
  - Abraxas
  - Agora Marketplace
  - Middle Earth Marketplace
  - Nucleus
  - Silk Road 1, 2 and 3
What is Tor?

- Acronym for The Onion Router
- Free software for enabling anonymous communication
- Originally developed on behalf of the U.S. intelligence community
- Today it is used by criminal enterprises, hacktivists, and law enforcement agencies
  - Users can remain anonymous
  - Activities can remain untraceable
  - Resources can remain hidden
How is Tor Accessed?
The Tor Browser

Congratulations!
This browser is configured to use Tor.
You are now free to browse the Internet anonymously.
Test Tor Network Settings

Search securely with Disconnect.me.

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

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

The Tor Project is a US 501(c)(3) non-profit dedicated to the research, development, and education of online anonymity and privacy. Learn more about The Tor Project »
How Does Tor Work?

Step 1: Alice’s Tor client obtains a list of Tor nodes from a directory server.
How Does Tor Work?

Step 2: Alice’s Tor client picks a random path to destination server. Green links are encrypted, red links are in the clear.
How Does Tor Work?

Alice

Step 3: If at a later time, the user visits another site, Alice's tor client selects a second random path. Again, green links are encrypted, red links are in the clear.

Dave

Jane

Bob

torproject.org
Accessing Underground Marketplaces

OnionDir - Deep Web Link Directory

dirkxdraygbifgc.onion - Your copy and paste friendly .onion link list. Feel free to copy this list to forums, pastebin etc so people can find hidden service links that actually work! You can add new links here, please check if the site is up before you add it, I will delete not working sites on a regular basis.

Categories:

Hidden Service lists and search engines
- http://mh67/rrzwbeinsl.onion/ - TORCH - Tor Search Engine
- http://32rfclwruor4f4iy.onion/ - Onion URL Repository
- http://e266al32vqordwp.onion/bookmarks.php - Dark Nexus
- http://5plv5sgyday2agc6.onion/ - Seeks Search
- http://2vlopcgqjhm5r2.onion/ - Gateway to Freenet
- http://nimymchmrnimnqi.onion/ - Is It Up?
- http://kpvvyyvymkxj7w2.onion/link.html - ParaZite
- http://wiktkauiduowq23.onion/ - Onion Wiki
- http://kpvz7kszylagwt35.onion/ - The Hidden Wiki
- http://dmocnkne4q756q.onion/ - Tor Project, Anonymity Online
- http://torlinkbgs6aatms.onion/ - TorLinks
- http://wikijerri4lgzd4.onion/ - Hidden Wiki - Tor Wiki
- http://wdagkmw73ayzth.onion/ - Anonet Webproxy
- http://3mb44arh09d2thl.onion/wik/index.php?title=Main_Page - All You're Wild - clone of the clean hidden wiki that went down with freedom hosting
What’s Sold on a Typical Tor Marketplace?

Source: Abraxas marketplace
Underground Marketplaces on Tor

- Typically require registration

- Some require invitation to join
  - Link on another site – not difficult to obtain

- Some marketplaces are sophisticated
  - Seller ratings
  - Seller profiles
  - Order history
  - Online discussions groups
Typical Tor Marketplace
Typical Tor Marketplace - Pirated Software
Typical Tor Marketplace - Luxury Goods
Typical Tor Marketplace - Pharmaceuticals
Typical Tor Marketplace - Counterfeits
Typical Tor Marketplace – Account Info

A screenshot of a Tor Marketplace interface showing listings for various items including bank accounts, digital goods, and BTC and DASH exchanges. The interface includes sections for fraud related, digital goods, listings, and BTC exchange. The bank account listings show various details such as name, price, shipping, and vendor.
So What Role Does Bitcoin Play?

- Sites utilize Bitcoin to conduct transactions
- Other types of cryptocurrency are sometimes accepted
  - Dash (formerly known as Darkcoin)
How Does Bitcoin Work?

- Anonymous payment system
  - Utilizes peer-to-peer technology to operate with no central authority
  - Relies upon “Miners” rewarded with Bitcoin to conduct network transactions
  - Transactions are conducted electronically using URIs which can be imbedded in QR codes for use with mobile devices

- Bitcoin can be bought and sold through online exchanges
  - Currently 13 million Bitcoin in circulation
  - Current value of a Bitcoin is ~$295 US
  - By 2140, there will be no more than 21 million Bitcoin
Features of Bitcoin

- **Decentralized**
  - The Bitcoin network is not controlled by any one central authority - every machine that mines Bitcoin and processes transactions makes up a part of the network, and the machines work together.

- **Anonymous**
  - Bitcoin addresses are not linked to names, addresses, or other personally identifying information.

- **Fast**
  - Money can be sent anywhere and arrives within minutes, as soon as the Bitcoin network processes the payment.

- **Non-Reversible**
  - When Bitcoins are sent, there’s no getting them back, unless the recipient returns them to you – they are gone forever.
Identifying Abuse in Deep Web

- Social Media
- Un-Indexed Websites
- Search Engines Ads
- P2P/ Filesharing
- Mobile Apps
- Email
- Market places
Mitigating Abuse in Deep Web

- Enforcement options
  - C&Ds to website operators
  - Take-down requests to ISPs
  - Notices to marketplaces, social media sites, mobile app stores
Identifying Abuse in the Darknet

- Understand your level of risk
  - FIs must be monitoring for account information
  - Those with counterfeiting issues should determine if these marketplaces provide means of mass distribution
  - All others should:
    - Determine whether you need regular monitoring OR
    - Periodic monitoring for changes to the threat landscape

- Track abuse over time
  - Evolving area of the Internet
Mitigating Abuse in the Darknet

- Due to anonymity, online enforcement difficult
  - May be information if seller profiles are available
    - E-mail addresses may be used to uncover additional information
  - May consider test-buys to understand what is being sold
    - Truly counterfeit, grey market, stolen

- For stolen account or credential information
  - Work with internal fraud teams to determine next steps
Questions?
Thank You!

- For information on MarkMonitor solutions, services and complimentary educational events
  
  - Contact us via email:
    field.marketing@markmonitor.com

  - Visit our website at:
    www.markmonitor.com

  - Contact us via phone:
    US: 1 (800) 745 9229
    Europe: +44 (0) 203 206 2220