The Zeitgeist of Darknet

OWASP Czech Chapter Meeting
14th November 2018

Ing. Martin Klubal
Senior IT Security Specialist
info@martinklubal.cz
Content

- Terminology
- Tor News in 2018
  - Next Gen Onion Services
  - Tor Browser for Android
- Statistics
- Vulnerabilities
- Seizure & Conviction
- Popular Hidden Services
- DEMO: Tor Real Hacking
Terminology

- **Clearnet/Surface web**
  - [https://www.google.com/](https://www.google.com/)
  - [http://crdclub.su/](http://crdclub.su/)

- **Darkweb (Darknet)**
  - Hidden Wiki
  - Silk Road

- **Deepweb**
  - Invite Only Sites
Next Gen Onion Services aka prop224

- Better crypto
- Improved directory protocol
- Better onion address security against impersonation
- More extensible introduction/rendezvous protocol
- A cleaner and more modular codebase
- Onion v3 Addresses
  - 56 characters long

vww6ybal4bd7szmngncyruucpgfkqahzdhi37ktceo3ah7ngmcopnpyyd.onion
Tor Browser for Android

- Google Play (Alpha)

- Alternatives
  - Orfox (don't use anymore)
  - Onion Browser (iOS)
Statistics

- Atlas – List of relays
  - https://atlas.torproject.org/
Statistics

The Zeitgeist of Darknet

Unique .onion addresses

The Tor Project - https://metrics.torproject.org/
Statistics

The Tor Project - https://metrics.torproject.org/
Statistics

Directly connecting users from the Czech Republic

The Tor Project - https://metrics.torproject.org/
Statistics

- Top 10 countries by relay users in 2018
- Germany 466948 (18.68 %)
- USA 403368 (16.14 %)
- UAE 292873 (11.72 %)
- Russia 250015 (10.00 %)
- France 102353 (4.10 %)
- Ukraine 98135 (3.93 %)
- Indonesia 83692 (3.35 %)
- UK 63145 (2.53 %)
- Netherlands 55173 (2.21 %)
- India 43275 (1.73 %)
Vulnerabilities

- Tor Browser 0-Day Exploit
  - version 7.x
  - vulnerability in the NoScript plugin
  - JavaScript execution in Safest Security Level
- Tor users deanonymization
  - patched in the latest branch 8.x

https://twitter.com/Zerodium/status/1039127214602641409
Vulnerabilities

- **Guard Discovery**
  - the most serious threat of the v3 onion services
  - lots of relays under the attacker control required
    - Hidden Services & Tor users deanonymization
  - Patched through the Vanguards Add-On
    - not a part of the Tor core yet

https://blog.torproject.org/announcing-vanguards-add-onion-services
SSL Certificate Deanonymization

14th November 2018

The Zeitgeist of Darknet
Vulnerabilities

- SSL Certificate Deanonymization
  - Use Shodan
- DigiCert.com issues trusted .onion certs
- SSL certs are **redundant** in Tor

https://twitter.com/ydklijnsma/status/1025796349541769217
Seizure & Conviction

- No significant Hidden Service seized
- Conviction
  - Gary Davis (Irish)
    - Silk Road admin
    - Pleaded guilty to drug trafficking (up to 20 years)
  - Gal Vallerius (French)
    - Dream Market admin
    - Pleaded guilty to drug trafficking/launder money (20 years)
Popular Hidden Services

- Dream Market
  - http://uffti3lhacanefgy.onion/
  - Black Market
  - online from November 2013
Dream Market

CZECH DL (physical, issued before 2017)

Vendor: LabDoc (0)
Price: $0.1239 ($780)
Ships to: Worldwide
Ships from: Worldwide
Escrow: Yes

Links
- Forum
- Help
- Conferences
- Vendor application
- Earn money
- Exchange
  - BTC
  - mBTC
  - BCH
  - USD
  - EUR
  - GBP
  - CAD
  - AUD
  - mBCH
  - BRL
  - DKK
  - NOK
  - SEK
  - TRY
  - CNY
  - HKD
  - PHP
  - INR
- News
  - New forum
  - Downtime & Recovery
  - Deposit delays
  - Status under maintenance
Popular Hidden Services

- The Hidden Wiki
  - [http://zqktlwi4fecvo6ri.onion/](http://zqktlwi4fecvo6ri.onion/)
  - Directory of Links
Main Page

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

Editor's picks

Pick a random page from the article index and replace one of these slots with it:

1. The Matrix - Very nice to read.
2. How To Exit The Matrix - Learn how to Protect yourself and your rights, online and off.
5. Terrific Strategies To Apply A Social media Marketing Approach - Great tips for the internet marketer.

Volunteer

Here are the six different things that you can help us out with:

1. Plunder other hidden service lists for links and place them here!
2. File the SnapDBSidebar links wherever they go.
3. Set external links to HTTPS where available, good certificate, and same content.
5. Perform Dead Services Detects.
6. Remove CP2 shleness.

Introduction Points

- Ahnlib.st - Clearet search engine for Tor Hidden Services.
- DuckDuckGo - A Hidden Service that searches the clearet.
- TorInks - TorInks is a moderated replacement for The Hidden Wiki.
- Torch - Tor Search Engine. Claims to index around 1.1 million pages.
- The Hidden Wiki - A mirror of the Hidden Wiki. 2 days old users can edit the main page.
Popular Hidden Services

- **Ahmia**
  - [http://msydqstlz2kzerdg.onion/](http://msydqstlz2kzerdg.onion/)
  - Fulltext Search Engine
Ahmia

Ahmia searches hidden services on the Tor network. To access these hidden services you need the Tor browser bundle. Abuse material is not allowed on Ahmia. See our service blacklist and report abuse material if you find it in the index. It will be removed as soon as possible.

For more about Ahmia, see indexing information, contribute to the source code.

The Tor Project

Onion service: msydostl2zkzerdg.onion

14th November 2018

The Zeitgeist of Darknet
Popular Hidden Services

- **ProtonMail**
  - https://protonirockerxow.onion/
  - Anonymous Freemail
  - Branch of ProtonMail.com
ProtonMail

The Zeitgeist of Darknet
Popular Hidden Services

- Daniel’s Hosting
  - http://dhosting4okcs22v.onion/
  - Webhosting
  - Most popular webhosting at the moment
    - 4002 public hosted sites
    - 1604 hidden hosted sites
      - Deepweb
      - Let’s hack it 😊
Thank you for your attention!

Any questions?