

Darknet Analysis

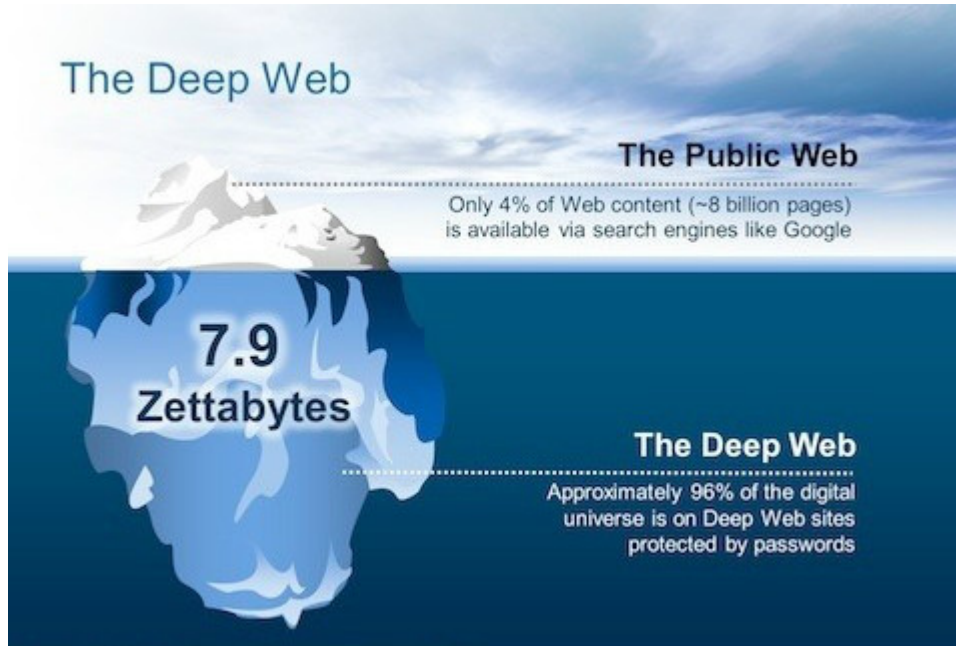
Peter KIESEBERG

Darknet Analysis

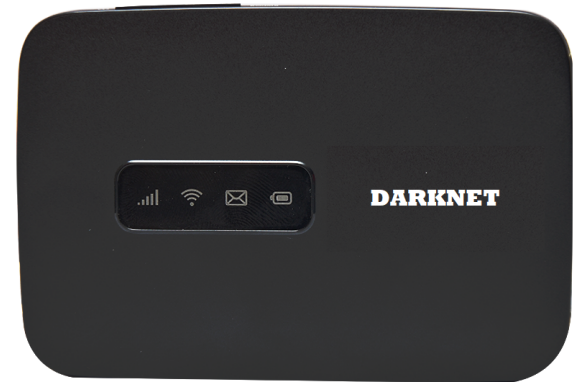
Privacy-aware automated analysis of underground marketplaces



The deep and the dark

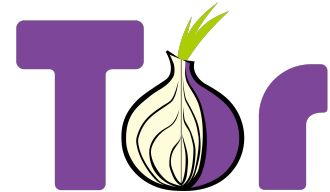


Taken from: <https://www.deepweb-sites.com/>



Underground marketplaces

- Trading places
 - Malware (e.g. Ransomware, Bot nets)
 - Weapons, Drugs ...
- Based on different technologies
 - Often TOR hidden services
 - Payment via Crypto-Currencies
- Famous example: Silkroad



Goals

- **Trends in the underground economy**
 - Automated analysis of underground marketplaces
- Four main targets:
 - Automated information retrieval
 - Privacy sensitive analysis
 - Data protection and legal issues
 - Analysis of underground marketplaces

Special requirements

1. Stealthy reconnaissance
2. Privacy protection
3. High degree of automation
4. Integration with existing tools and workflows

Non-Goals

- De-anonymization of TOR-traffic
- Linking hidden services to actual places
- Taking down marketplaces
- Comprehensive analysis of the market

Solution approach

- Iterative approach
- Several complete overhauls
- Including structure
- Reducing size to app. 50 pages

Special Focus: Automation

Core issue: Providers of UMs try to detect reconnaissance

- Source detection & generation
- Solving Captcha
- Automated profile generation
- Simulating user behavior

Privacy sensitive analysis

Core issue: Provide analytical methods that respect privacy

- Study on the effects of anonymization on ML
- Privacy by Design in the reconnaissance process
- Trends versus detailed analysis
- PAML

Data Protection

- Core issue: Protect the data collection for use as evidence.
- Audit & Control
- Manipulation Detection
- Traceability

Partners

- SBA Research
- TU Graz
- University of Vienna (GSK)
- Bravestone GmbH
- BM.I
- BMLV



Peter Kieseberg
Research Coordinator

SBA Research gGmbH
Favoritenstraße 16, 1040 Vienna
+43 660 312 6291
pkieseberg@sba-research.org



Competence Centers for
Excellent Technologies

