##1 A Focused Crawler for Dark Web Forums

Tianjun FuDepartment of Management Information Systems, University of Arizona, Tucson, AZ 85721.E-mail: futj@email.arizona.eduAhmed AbbasiManagement Information Systems, Sheldon B. Lubar School of Business, University ofWisconsin–Milwaukee, Milwaukee, WI 53201. E-mail: abbasi@uwm.eduHsinchun ChenArtificial Intelligence Lab, Department of Management Information Systems, University of Arizona,Tucson, AZ 85721. E-mail: [*hchen@eller.arizona.edu*](mailto:hchen@eller.arizona.edu)

Several URL ordering features and techniques enable efficient extraction of forum postings.The system also includes an incremental crawler coupled with a recall-improvement mechanism intended to facilitate enhanced retrieval and updating of collected content. Despite the need for tools to collect and analyze Dark Web forums, the covert nature of this part of the Internet makes traditional Web crawling techniques insufficient for capturing such content. The human-assisted approach significantly improved access to DarkWeb forums while the incremental crawler with recall improvement also outperformed standard periodic- and incremental-update approaches. A case study encompassing link and content analysis of collected forums was used to illustrate the value and importance of gathering and analyzing content from such online communities. The system uses a human-assisted accessibility approach to gain access to Dark Web forums. In this study, we propose a novel crawling system designed to collect DarkWeb forum content.

##2 Focused crawling for the hidden webPanagiotis Liakos1 · Alexandros Ntoulas ·Alexandros Labrinidis3 · Alex Deli

In order to excavate and make available meaningful data from the Hidden Web, previous work has focused on developing query generation techniques that aim at downloading all the content of a given Hidden Web site with the minimum cost. We investigate how we can build a focused Hidden Web crawler that can autonomously extract topic-specific pages from the Hidden Web by searching only the subset that is related to the corresponding area.

##3Darknet and Deepnet Mining for Proactive Cybersecurity Threat Intelligence.

Eric Nunes, Ahmad Diab, Andrew Gunn, Ericsson Marin , Vineet Mishra,  
Vivin Paliath, John Robertson, Jana Shakarian, Amanda Thart, Paulo Shakarian  
Arizona State University  
Tempe, AZ 85281, USA  
Email: fenunes1, ahmad.diab, andrewgunn, ericsson.marin, vvmishra,  
vivin.paliath, jj.robertson, jshak, amanda.thart, shakg @asu.edu

In this paper, we present an operational system for cyber threat intelligence gathering from various social platforms on the Internet particularly sites on the darknet and deepnet. We have developed an operational system for obtaining information from these sites for the purposes of identifying emerging cyber threats. We focus our attention to collecting information from hacker forum discussions and marketplaces offering products and services focusing on malicious hacking. With the use of machine learning models, we are able to recall 92% of products in marketplaces and 80% of discussions on forums relating to malicious hacking with high precision.

##4 Policing the Dark Web: Ethical and Legal Issues  
*Kat Hadjimatheou*

University of Warwick and TNO

1. Key recommendations emerging from this section include that LEAs should develop supplementary, detailed guidance for authorizing and covert officers doing operations on the Dark Web in order to ensure that they are carried out in ways that are necessary and proportionate; that the effectiveness of tactics and operations should be monitored systematically by LEAs over time to create the kind of evidence base on which best practices could be developed- Interpol could have an important role to play in facilitating this at an international level; LEAs should be as transparent as possible about the outcomes of operations and how these constitute effectiveness and efforts should be made to develop evaluation techniques that can measure the currently undervalued disruption effects of methods and operations.
2. In order to ensure their relevance, the ethical and legal issues considered in this report are discussed with reference to two recent real-life LEA operations on the dark web: Operation Bayonet, which involved the takedown by LEAs of Dark Web marketplaces AlphaBay and Hansa, and Task Force Argos, an Australian anti-CSE LEA unit which involved the infiltration and running of the notorious Dark Web CSE forum ‘Child’s Play’.
3. With respect to LEA operations, which are the focus of the first half of the discussion, the report addresses the following two questions: What, if any, kinds of methods or tactics should police be prohibited from using when tackling crime on the Dark Web?’ and ‘What considerations should guide police decisions with respect to using methods that may not be prohibited, but are nevertheless seriously harmful?’ The report considers a range of relevant harms, from the re-victimisation of children, to harms to officer welfare, to interference with the exercise of freedom of expression and association online.