The Dark Web: Defined, Discovered, Exploited

Stephen Mancini, National Cyber-Forensics & Training Alliance, USA
Lawrence Tomei, Robert Morris University, USA

ABSTRACT

The Dark Web is its own clandestine network of thousands of websites that most of us do not even know exist, much less how to access. The Dark Web uses its own tools to keep users anonymous and their activities hidden. The Dark Web is so well concealed that the full extent of its use remains largely the topic of hushed conversations. From black market drug sales to child pornography, the Dark Web operates at two extremes of the Internet, from venues for anonymous whistleblowing on one end to unguarded censorship on the other. This article provides a primer for those interested in learning more about the “known unknowns” of the Dark Web. Readers will find an excellent opening manuscript for the newly launched International Journal of Cyber Research and Education as it sets the stage for future research in cyber security and law enforcement. The paper will examine three foundational questions for the reader: What constitutes the ‘deep/dark/underground’ web and keeps it obscure and remote from the community of legitimate users? How can websites that occupy the same virtual space range exist in two parallel dimensions from discoverable to undiscoverable? And finally, how do the actors on the Dark Web mature from novice to advanced? Is it the same process followed by users of the known web? In the corpus of this article, the authors will briefly examine how online markets exist simultaneously on the Internet, serving clients in both known online environments as well as the more secretive, anonymous online world. They will examine how nefarious actors migrate from the “good” web to become novice and then advanced users of the “evil” environments. To the neophyte user, the process introduced herein may appear relatively straightforward. In truth, the notion that any but the most staunchly dedicated practitioner can become a vetted participant in the ‘dark web’ is inconceivable. Even so, with the sheer volume of actors operating in numerous underground forums and marketplaces, the impact remains significant and growing geometrically. Government and industry from all over the globe are hindered in their ability to track and identify the truly advanced actors operating in these more secretive environments. We shall soon see why this is the case.

KEYWORDS
Dark Web, The Onion Router (TOR), Underground Forums, Underground Marketplaces

INTRODUCTION

In 2002, Secretary of Defense, Donald Rumsfeld responded to a media inquiry regarding ongoing activity in the early days of the Iraq war with the now-infamous line, “…there are known knowns; there are things we know we know. We also know there are known unknowns; that is to say, we know there are some things we do not know…” While there is much discussion and research regarding the

DOI: 10.4018/IJCRE.2019010101
Dark Web, the reality is that the average Internet user is either unaware or unable to reach many of the more secretive locations of the internet. For those that are aware of them and able to locate them, it is probably because they are seeking to conduct illegal dealings, with the exception of researchers and law enforcement who are there to identify those attempting to conduct illicit activity. The additional challenge is the number of individuals participating in these more secretive environments continues to rise as it is becoming easier for novice and intermediate actors to participate in some capacity. For example, the web site www.deepdotcom.com provides a daily update on the availability of current underground forums and marketplaces as well as tutorials on best practices for accessing these sites in a more secure manner while ensuring anonymity. This creates a challenge; a large number of nefarious actors operating in an environment with only a limited number of ‘good guys’ trying to determine who’s who. For example, the AlphaBay and Hansa marketplaces which sold various illegal commodities were recently taken down by law enforcement. On AlphaBay, the National Cyber Forensics and Training Alliance (NCFTA) was able to identify roughly 875 vendors with a seller’s rating of 4 or more out of 10. They were sellers of illegal commodities who were fairly well reviewed by buyers. On Hansa, roughly 600 vendors with a rating of 4 out of 10 were identified. Assuming even a 30 percent overlap in these individuals being persons in both marketplaces, that would mean there are roughly 1,000 individual vendors operating in just these two marketplaces. Considering it takes years to build a cyber case, especially if there are international connections, the reality of law enforcement ability to impact the online nefarious activity of such individuals remains a significant and growing challenge. For example, Evgeniy Bogachev remains the FBI’s most wanted cybercriminal with a $3M USD bounty for information leading to his capture. It took years and multiple agents to identify him but as he is likely operating out of Russia, he will apt to continue with relative impunity. Compounded by the fact that every day nefarious actors from all over the world are entering into these marketplaces and forums and thus increasing their skill set.

**DEFINED – WHAT IS THE DARK WEB?**

In its early days, the Internet was little more than a promising set of interconnected university and government sites, accessed through command line instructions on machines over something called ARPANET. ARPANET, a research project funded by the Advanced Research Projects Agency, was the predecessor of the Internet with “…the goal… to exploit new computer technologies to meet the needs of military command and control against nuclear threats, achieve survivable control of US nuclear forces, and improve military tactical and management decision making.”1 It was not until the early 1980s, with the introduction of the TCP/IP standard that the roots of the modern-day Internet began. In roughly 25 years, the Internet went from its first Graphical User Interface (GUI) based browser with a few colors and some midi music tapping a few beats in the background to a network that spans the globe encompassing billions in US dollars in ecommerce and allowing live news, music and other media to be streamed from anywhere. Most importantly, it created an environment that allows for endless forms of collaboration between essentially any individual in the world with access. While this has allowed humanity to increase its knowledge positively and exponentially, it has also enabled users with less than noble purposes to increase their knowledge and skillsets as well.

Early collaboration typically existed with small groups of very technical users communicating through mechanisms such as dial up bulletin boards (BBS) or internet relay channels (IRC). Today, there are numerous online forums which enable various topics for discussion, with easy to understand domain names, such as hxxp://www.Reddit.com, operating within the well-known internet top level domains (.com, .org, .edu, etc.) to specialized sites requiring certain tools to access; some of the more common being .onion sites requiring TOR or .i2p requiring the i2p app.

TOR was first developed by the US government, and has since been maintained and updated by the TOR project-- a group whose purpose is to ensure users can safely and anonymously browse the internet. This anonymity creates opportunity, not just for an individual living in an oppressive society,
Probabilistic Evaluation of SMS Messages as Forensic Evidence: Likelihood Ratio Based Approach with Lexical Features
www.igi-global.com/chapter/probabilistic-evaluation-sms-messages-forensic/75669?camid=4v1a