James Madison Undergraduate Research Journal

Volume 5 | Issue 1

2017-2018

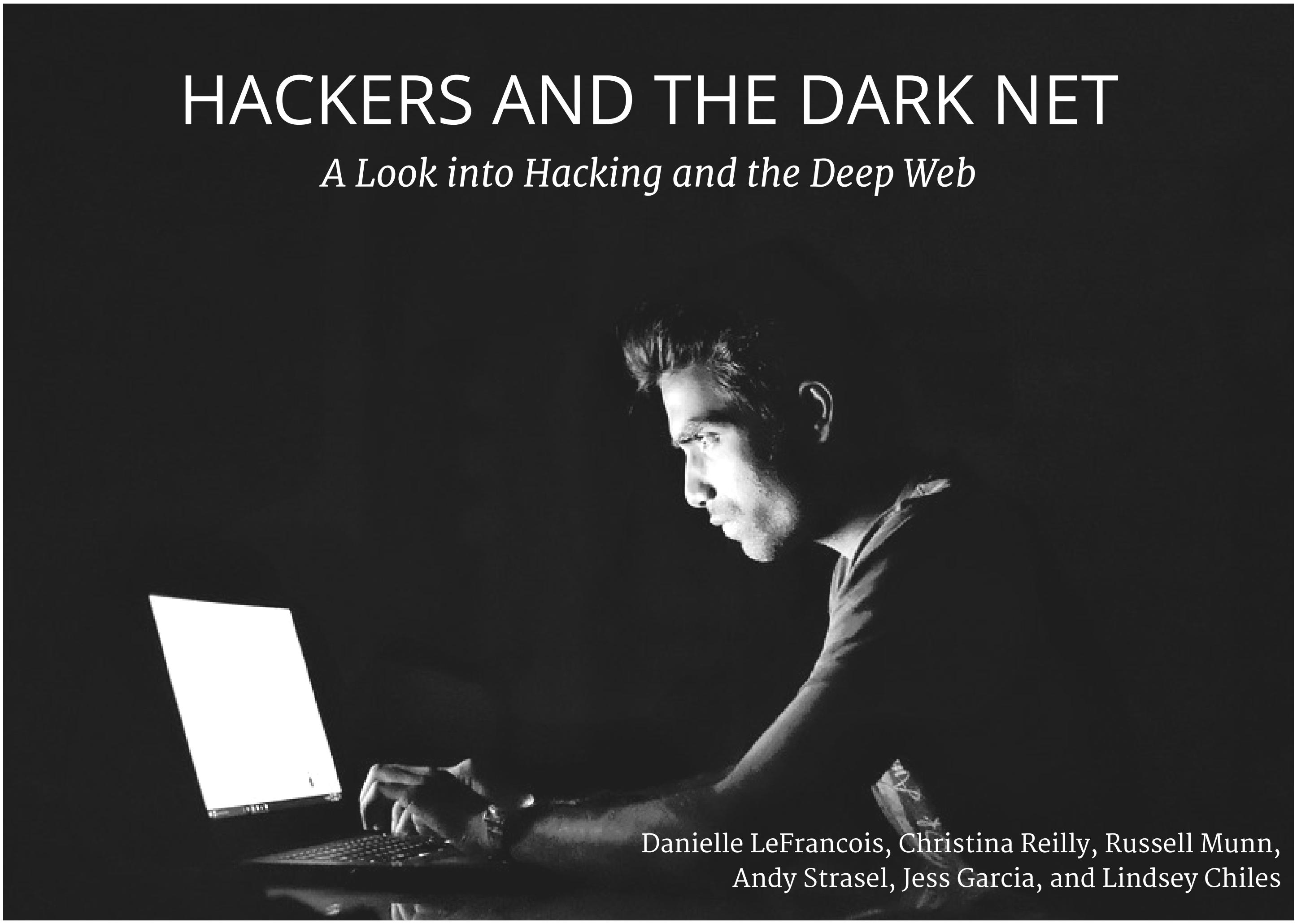
Hackers and the Dark Net: A Look into Hacking and the Deep Web

Danielle LeFrancois, Christina Reilly, Russell Munn, Andy Strasel, Jess Garcia, and Lindsey Chiles

James Madison University

HACKERS AND THE DARK NET

A Look into Hacking and the Deep Web



Danielle LeFrancois, Christina Reilly, Russell Munn,
Andy Strasel, Jess Garcia, and Lindsey Chiles

ABSTRACT

The dark web is notorious for the illicit activities it facilitates, including human trafficking, narcotics and weapons sales, and illegally obtained information transfers. In order to combat this constant, invisible threat to security, governments and experts have called for tougher legislation and increased surveillance. But on the opposite end of all this crime and villainy lie persecuted groups who use the dark web and the anonymity it affords to protect themselves from retaliation. This article uses Atavist's digital storytelling medium to explore how hackers "hack" the web, ethical questions surrounding the dark web, and policy solutions to cyber security.

To view the article, visit https://smad470.atavist.com/hackers-and-the-dark-net.

EDITORS' NOTE:

JMURJ is proud to present its second multimedia piece, "Hackers and the Dark Net," by a team of Media Arts & Design students. We have offered a brief exerpt here. The full work, created on Atavist, is available at the link below.

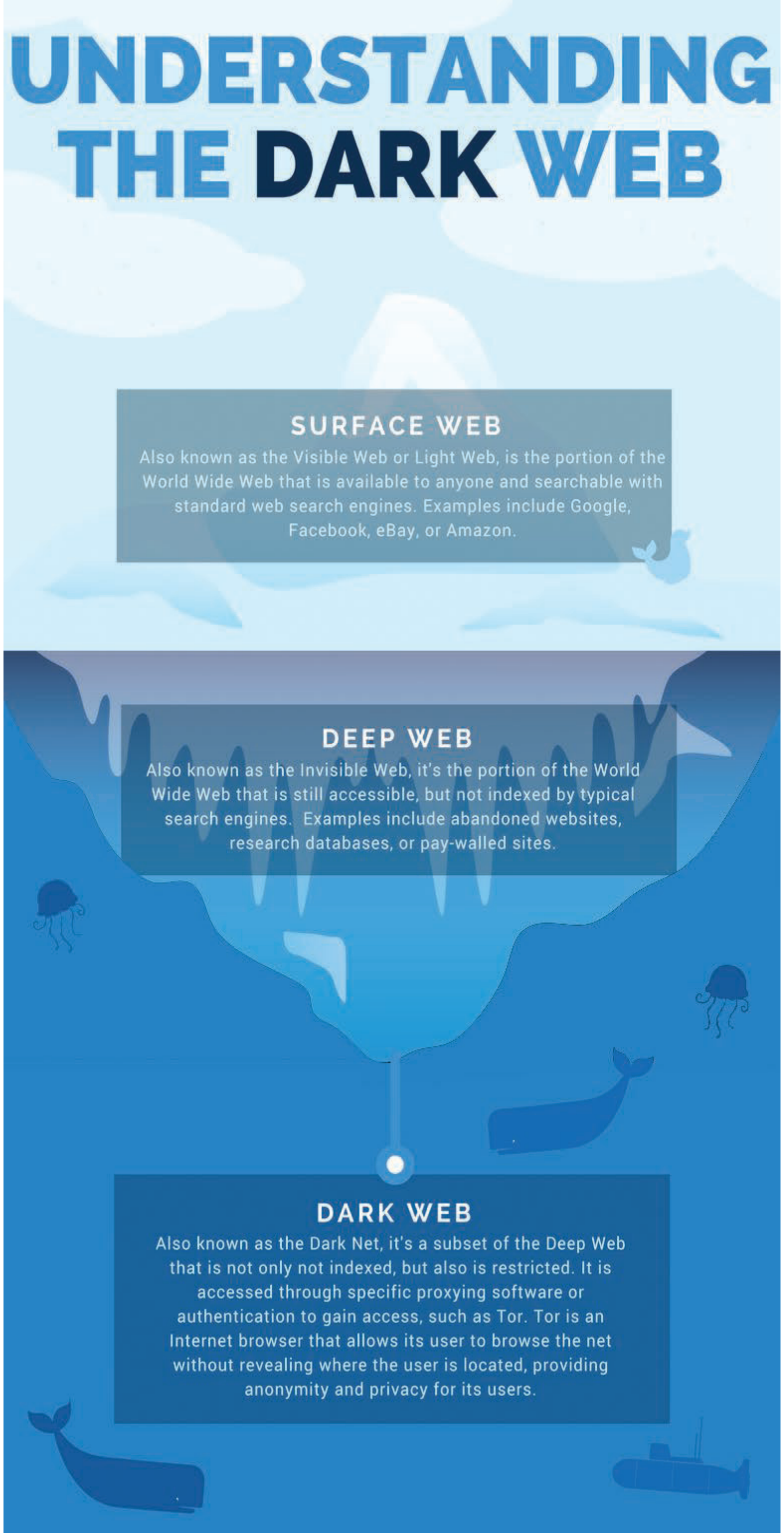
OVERVIEW

Vastly larger than the usual "surface" Web that the typical user is familiar with, the Dark Net is the gathering place for all those Internet- and tech-savvy individuals who prefer their anonymity. Accessed primarily by the free-to-download Tor browser, which routes connections through multiple server networks and sometimes across continents, the Dark Net allows anyone who has the appropriate know-how to find and use spaces to a multitude of ends. Popular stock on the Dark Net includes weapons, child pornography, drugs, malware, stolen credit card details, and pirated movies and music, all paid for by the anonymity-protecting digital currency Bitcoin.

In addition to goods and services, the Dark Net also allows groups to communicate without worrying about the authorities intercepting their messages or discovering the identities of members. Groups like ISIS and organized crime cells use the Dark Net to recruit, plan, and collaborate. And, as soon as the authorities shut down a Dark Net site—if ever—another equally, if not more difficult to locate, site appears instantaneously.

In order to combat this constant, invisible threat to security, governments and experts call for tougher legislation and increased surveillance. But on the opposite end from all this crime and villainy lie persecuted groups who use the Dark Net and its offer of anonymity to protect themselves from retaliation. Ethnic minorities, religious groups, and political activists are able to exercise their rights to freedom of expression and speech as well as organize and support one another without the fear of being exposed or endangered for their beliefs.

VIEW HERE



UNDERSTANDING THE DARK WEB

SURFACE WEB

Also known as the Visible Web or Light Web, is the portion of the World Wide Web that is available to anyone and searchable with standard web search engines. Examples include Google, Facebook, eBay, or Amazon.

DEEP WEB

Also known as the Invisible Web, it's the portion of the World Wide Web that is still accessible, but not indexed by typical search engines. Examples include abandoned websites, research databases, or pay-walled sites.

DARK WEB

Also known as the Dark Net, it's a subset of the Deep Web that is not only not indexed, but also is restricted. It is accessed through specific proxying software or authentication to gain access, such as Tor. Tor is an Internet browser that allows its user to browse the net without revealing where the user is located, providing anonymity and privacy for its users.