Business Horizons (2016) xxx, xxx—xxx

Available online at www.sciencedirect.com

ScienceDirect

KELLEY SCHOOL OF BUSINESS
INDIANA UNIVERSITY

www.elsevier.com/locate/bushor

The looming shadow of illicit trade on the internet

Peggy E. Chaudhry

Villanova School of Business, Villanova University, 800 Lancaster Avenue, Villanova, PA 19085, U.S.A.

KEYWORDS
Darknet;
Internet piracy;
Malvertising;
Crimeware;
Ransomware;
Online black market;
Cybercrime prevention

Abstract Pirates on the virtual sea are supplying their illicit digital content and goods through cyberlockers and darknet markets. The deep web hosts darknet marketplaces selling a variety of wares, such as narcotics and weapons, and is testimony to the growth of illicit trade on the internet. The challenge of web sites that host digital content piracy is exacerbated through linkages to a variety of malware schemes that have created a lucrative crimeware economy. Digital thieves target unsuspecting consumers as digital bait to derive profits from a variety of malware schemes such as ransomware and malvertising. The hijacking of access to computers and their digital content in order to ransom them back to consumers or organizations is considered to be one of the leading threats of internet crime. Malvertising schemes are plaguing the internet advertising business—criminals are reaping profits by posting legitimate advertisements at content theft sites or using an army of botnets to fake advertising traffic. A variety of stratagems are evolving to curb this illicit trade, including fostering multi-lateral enforcement tactics, updating legislation to circumvent this type of crime on the internet, training digital savvy citizens, and creating private-sector remedies.

1. The Wild West of cyberspace

Two decades ago, Barry James (1996) characterized the internet as a "Wild West frontier town without a sheriff" and warned consumers about web services that offered bogus stock, other spurious schemes involving, for example, gold mines, gemstones, and ostrich farming, and even the possible loss of identity by way of email addresses and credit card numbers. The issue of pirated digital content and counterfeit merchandise obtained via the internet has been studied for over 2 decades with key sectors examined, including music, movies, software, and pharmaceuticals (Chaudhry, 2013; Chaudhry, Cesareo, & Stumpf, 2014). But, the continued global growth of consumer access to broadband and the use of several devices to access illicit digital content is fueling the growth for this type of illicit trade (Sudler, 2013).

To illustrate the progression of internet piracy, the top pirated movie in 2011 was *Fast Five* with an

E-mail address: peggy.chaudhry@villanova.edu

0007-6813/$ — see front matter © 2016 Kelley School of Business, Indiana University. Published by Elsevier Inc. All rights reserved.
http://dx.doi.org/10.1016/j.bushor.2016.09.002

estimated 9.26 million downloads via a torrent site, a file sharing network and system often used to distribute pirated media (Chaudhry & Zimmerman, 2013). Four years later, *Interstellar* topped the 2015 piracy list with 46.8 million downloads (BBC News, 2015). TorrentFreak.com lists the top weekly pirated movies complete with each movie's IMDb.com rating and trailer; *Warcraft* topped the chart on July 3, 2016 (Ernesto, 2016). The illicit digital content of a movie on the internet can stem from a variety of sources: images taken in the theater using a camcorder or mobile phone (i.e., a CAMrip), a copy of an uncut version of the movie from the studio (i.e., a workprint), a copy of the retail version of the DVD or Blu-Ray DVD (i.e., a DVD Full-Rip or BRRip), or a file copy from a DRM-free streaming service like Hulu (i.e., a WEBRip).

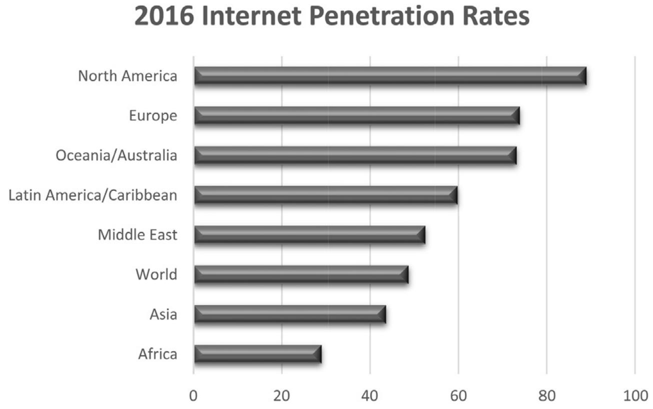
Pirates on the virtual sea continue to use different infringement ecosystems to supply illicit digital content and counterfeit goods: BitTorrents, cyberlockers, and darknet markets (NetNames, 2014). Chaudhry and Stumpf (2013) reported on the struggles of fake pharmaceuticals sold on the internet, but even more reprehensible are the Amazon-like marketplaces on the darknet selling other illicit goods such as narcotics and weapons. Consumers who visit these nefarious sites are exposed to other criminal activities like identity theft through malware and are lucrative digital bait for cybercriminals (Digital Citizens Alliance, 2015a). In July 2016, the limited geographic distribution of the new mobile game Pokémon GO created the opportunity for cybercriminals to serve unmet consumer demand by way of third-party websites. An unsuspecting Android consumer who side-loaded this game from a third-party website may have been infected with a Droidjack, a remote access control Trojan virus that gives total control over the mobile phone to the architect of the malware (Morris, 2016). The Business Software Alliance (2016) established significant linkages between installing illegitimate software and malware: the analysts discovered 430 million new pieces of malware in 2015, an increase of 36% from 2014. The internet advertising industry is struggling currently with 'malvertising' schemes that profit criminals either through the sale of advertisements that are posted on content theft sites and/or the use of an army of botnets to click repeatedly on advertising links to generate revenues.

In this article, the problem of illicit trade on the internet is addressed in the context of raising awareness about the threats and actions taken by a variety of stakeholders to mitigate this unlawful trade on the web. The main contributions advanced of this article involve: illustrating the significant growth of internet traffic for both fixed-access and mobile platforms to participate in both licit and illicit trade; describing the evolution of illicit supply chain ecosystems such as cyberlockers and darknets; recounting current malware schemes in the crimeware economy, specifically malvertising and ransomware, that ensnare unsuspecting consumers and employees of organizations as digital bait; portraying the criminal engineers involved and their ability to garner windfall profits; and discussing an array of stratagems to diffuse this trade that have been undertaken by enforcement agencies, government organizations, and companies.

2. Escalating demand for the internet

The size of the digital universe is measured in terms of the growth of internet penetration, the increased speed of bandwidth, and the number of devices used to access digital content. The Internet World Stats (2016) categorizes regions by internet penetration rates as a percent of total population. Figure 1

Figure 1. World internet penetration percentage rates by geographic region



Source: Internet World Stats (2016)