Baraton Interdisciplinary Research Journal (2018), 8(Special Issue), pp 1-7

THE DARK WEB AND CRYPTOCURRENCIES: A "TRUST" DILEMMA FOR DIGITAL COMMERCE?

Nyamwamu Rosaline* & Onsongo Nyamwaya
University of Eastern Africa, Baraton, P. O. Box 2500-30100, Eldoret, Kenya
*Corresponding author: Email address - rose@ueab.ac.ke

Abstract

The dark web is a layer of the internet that is encrypted and not accessible via ordinary browsers. It offers users the ability to securely and anonymously access the internet without being traced. This is accomplished via tools created through the Tor project. The dark web contains legal resources (32%)such as forums, radio service and illegal (68%) resources/ materials such as the avenue for blackmarket activities including selling drugs, child pornography, malware servers, assassination services etc. With the growth in the digital commerce, the dark web poses a threat to the core of what enables business "trust". Companies running digital commerce platforms need to offer assurances of trust and security to their clients as a way of instilling confidence in them and as a competitive advantage. This paper uncovers threats posed by the dark web to conventional digital commerce markets and proposed ways of mitigating them.

Keywords: Dark web, digital commerce, cryptocurrency, security

Introduction and Literature Review

The Web can be divided into two main parts which are the surface web and the deep web. The "surface Web" is the part of the web that people use routinely. It consists of data that search engines can find and when offer up in response to queries. Search engine sees about 0.03 percent of the information that is available and much of the rest of the information is submerged in what is called the deep Web (Bergman, 2001).

Paganini (2012) compares the deep Web to searching on the Internet today to dragging a net across the surface of the ocean: a great deal may be caught in the net, but there is a wealth of information that is deep and therefore missed. Also known as the "Undernet," "invisible Web" and the "hidden Web," it consists of data that cannot be located with a simple Google search (Chertoff & Simon, 2015).

Barker and Barker (2013) denotes the deep Web as simply, the part of the Web that is hidden from view. It is WWW content that is not part of the surface Web. It cannot be accessed by normal search engines. This massive subsection of the Internet is more than 500 times bigger than the visible Web. Most of the content located in the deep Web exists in websites that require a search that is not implicitly illicit. However, an intensive search using specific softwares can help one find the dark Web which is a small portion of the deep Web that has been intentionally hidden. The dark Web is also the preferred channel for governments to exchange documents secretly, for journalists to bypass censorship of several states and for dissidents to avoid the control of authoritarian regimes (Gehl, 2014).

The Internet is the tool that has made digital commerce grow at a geometrical rate in the 21st century. Businesses rely on the Internet as a tool to expand digital commerce, hence increasing markets in the search of accomplishing their mission. Unlike the "brick and mortar" businesses, in this age the Internet has woven a tapestry of business variety, and the transactions that businesses can carry out over the Internet are basically unlimited. Hence, the proliferation of the Internet has been a great opportunity for growth for every industry in the current business environment and more so for digital commerce. With a lot of information being transmitted and shared over the digital media, the issue of trust raises eye brows to both the e-vendors and e-customers. In this context trust means reliance on the integrity, ability, etc. of a person or thing.

Digital commerce utilizes electronic media to share information and make transactions. Thus, digital commerce through the Internet offers various profit opportunities. Firstly, the potential for a larger market exists by tapping into the vast internet user base. The

Internet also offers the possibility of lowering marketing and transaction costs thus increasing marginal revenue. Thus, the internet is a tool that provides digital commerce a greater outreach. The importance of trust on digital commerce cannot be underrated. Internet vendors and consumers are bounded by trust.

In Kenya, the Communications Authority of Kenya issues a fresh warning to all phone users in the county involving international calls where phone users receive very brief calls or missed calls from foreign numbers and are unknowingly directed to premium numbers that drain lines of credit. The scammers purchase the phone numbers used in the scam from the Dark web (Kejitan. 2018).

The main objective for the e-vendors is to provide an environment where e-customers can trust and feel secure enough to share information, cooperate and purchase. The e-customer wants the e-vendor to behave and act in the e-consumer's interest, by being "honest in transactions, and both capable of, and predictable at, delivering as promised" as indicated by Balasundram, Naranjo, and Subramaniam (2012). The anonymity of the dark web, thus raises an issue of trust.

Digital commerce vendors should enable e-consumers' control. E-consumers need products, services, systems and modes of living that provide convenience and saves time. Businesses value trust, for it helps both entities defeat barriers and makes trade and interactions easier. Trust helps business to grow by promoting positive experiences. Hence e-consumers need to feel secure and safe for them to build trust.

Objectives

This paper has the following objectives:

1. To examine threats posed by the dark web to digital commerce
2. To explore how trust can be retained on digital commerce sites

Defining Attributes

What is Digital Commerce?

Gartner (cited in Gillespie et al., 2017) defines digital commerce as the buying and selling interactions among businesses, people and things for products/services via digitalization technologies. These interactions result in valued transaction to the customer, based on a combination of factors, including good customer experience, inexpensive price, timeliness, ease of use, clear policies and others. Businesses have a common mission in a free market environment, which is to be profitable and earn positive return of equity and increase the value of the firm in the long run.

The Dark Web

The term deep Web is used to denote a class of content on the Internet that, for various technical reasons, is not indexed by search engines. The dark Web is a part of the deep Web that has been intentionally hidden and is inaccessible through standard Web browsers such as chrome. A relatively known source for content that resides on the dark Web is found in the Tor network. Tor, and other similar networks, enables users to traverse the Web in near-complete anonymity by encrypting data packets and sending them through several network nodes, called onion routers. Onion routing is a technique for anonymous communication over a computer network. Messages are repeatedly encrypted and then sent through several network nodes, called onion routers. This technique prevents intermediary nodes from knowing the origin, destination and contents of the message (Tor Project cited in Chertoff & Simon, 2015).

What is Cryptocurrency?

Cryptocurrencies are digitally coded scripts that attempt to replicate the government-backed currencies we use today. However, while transactions in government-backed currencies are tracked by central clearing houses or banks, cryptocurrency transactions are tracked by blockchain, a publically-viewable, digital ledger. The backbone of the cryptocurrency network is made up of 'miners': individuals or syndicates who use highly-efficient networks of computers to solve complex mathematical sequences in exchange for transaction fees and, in some cases, newly created cryptocurrency (UBS, 2017).

Payment on the Dark Web

Payment on the dark web are done using concurrency such as the Bitcon. It is a decentralized digital currency that uses anonymous, peer-to-peer transactions. Individuals generally obtain bitcoins by accepting them as payment, exchanging them for tra-

ditional currency, or "mining" them (Paganini, 2012). The use of cryptocurrencies on the dark web enables direct and anonymous transactions without oversight. These technologies enable online vendors and buyers to communicate and exchange funds anonymously and with little risk of detection.

When a bitcoin is used in a financial transaction, the transaction is recorded in a public ledger, called the block chain. The information recorded in the block chain is the bitcoin addresses of the sender and recipient. An address does not uniquely identify any particular bitcoin; rather, the address merely identifies a particular transaction.

Users' addresses are associated with and stored in a wallet. The wallet contains an individual's private key, which is a secret number that allows that individual to spend bitcoins from the corresponding wallet, similar to a password. The address for a transaction and a cryptographic signature are used to verify transactions. The wallet and private key are not recorded in the public ledger; this is where Bitcoin usage has heightened privacy. Wallets may be hosted on the web, by software for a desktop or mobile device, or on a hardware device.

The fact that every transaction in the Bitcoin blockchain is publicly available means investigators can examine them. Tracking money as it moves through the system is thus doable, albeit quite difficult. As a result, a number of services that add further anonymity to the system have surfaced, making the electronic currency even more difficult to track. This is generally achieved by "mixing" your Bitcoins—transferring them through a spidery network of micro-transactions before returning them to you. In the process, you end up with the same amount of money (normally, minus a small handling fee) but your transactions become substantially harder to track.

Threats to Digital Commerce

Gemalto's cybersecurity report (2014) says that many of companies' assets are at risk to criminal activities facilitated by the dark web, some of which criminals are actively vying to buy and sell. Some digital commerce assets at risk include: general and specific cyber exploits and vulnerabilities; intellectual property, designs and counterfeits; financial information including credit cards and banking details; and personally identifiable information. Details for some of these risk as discusses below:

Hacking

The dark web provides an environment for experienced hackers who coordinate sophisticated attacks or cyber-criminals such as purchasing hacking kits, stealing credit card and identity information to be auctioned to the highest bidder, the trafficking of stolen and counterfeit goods, and some forms of money laundering, often involving bitcoin or crytocurrencies also take place. It should be noted that "many countries, including the US, still use credit cards based on a magnetic strip that are quite easy to clone; the lack of security chips aids cyber criminals," according to the InfoSec Security Institute. It is correct to assume that dedicated sites facilitate users to trade in both physical and proprietary information, including passwords and access to passwords for surface Web paid-pornography sites and PayPal passwords (Westin, 2014). PayPal Store, Credit cards for All and (Yet) Another Porn Exchange are active websites that offer such services.

Dead Platforms

In the digital world, companies go under and often take their customers and investors with them. As the user of a digital currency, you fall under their customer base - and if the platform goes under, then your digital currency goes with it.

Illegal Financial Transactions

Websites such as Banker and Co. and Insta-Card offer illegal financial transactions such as facilitating untraceable financial transactions through various methods. They either launder bitcoins by disguising the true origin of the transactions or give users an anonymous debit card issued by a bank. Users are also given virtual credit cards issued by trusted operators in the dark Web (Dean, 2014).

Identity Theft

Credit card and identity information is available on the dark web on illegal websites to be auctioned to the highest bidder. Delamaire, Abdou, and Pointon (2009) lament that "Online merchants are at risk because they have to offer their clients payment by credit card. In cases where fraudsters use stolen or manipulated credit card data the merchant loses mon-

ey because of so-called 'charge backs'. In December 2016, a severe security vulnerability was discovered on a large online retailers' shopping platform in China. As a result, card numbers, login IDs, passwords, phone numbers and email addresses (PWC, 2017).

Illegal Underground Ecosystems

Within the dark web there are underground ecosystems that represent a portion of cyberspace that is considered vital for criminal communities, where criminals can acquire and sell tools, services and data for various kinds of illegal activities. The term underground ecosystem is usually used to refer a collection of forums, websites and chat rooms that are designed with the specific intent to advantage, streamline and industrialize criminal activities. Here, criminal crews offer any kind of documentation that could be used in sophisticated frauds. This would include passports, driver's licenses, social security numbers and even utility bills are commonly exploited by hackers as a second form of authentication by service providers. For this reason they are purchased by criminals in the dark net.

Anonymous Marketplaces

There are anonymous marketplaces where e-vendors can purchase anything. Examples of such Websites are Silk Road. Sold items range from books and clothes, to more illicit goods such as drugs and weapons. Aesthetically, these sites appear like any number of shopping websites, with a short description of the goods, and an accompanying photograph (Bartlett, 2014).

Mitigating Threats to Digital Commerce

Customer Data Monitoring

Security agencies could benefit from analyzing customer Web data to look for connections to non-standard domains. Depending on the level of Web usage at the customer side, this may not help in tracking down links to the dark Web, but it may still provide insights on activities hosted with rogue top-level domains. This can be done without intruding on the user's privacy as only the destinations of the Web requests need to be monitored and not who is connecting to them.

Marketplace Profiling

Security agencies should use profiling software so as to profiling transactions made on dark Web marketplaces which would indicate information about sellers, users and the kinds of goods exchanged. Individual profiles could be built up over time.

Hidden Service Monitoring

Since most hidden services to tend to be highly volatile and go offline very often, coming back online later under a new domain name, it is essential to get a snapshot of every new site as soon as it is spotted, for later analysis or to monitor its online activity. While crawling the clear Internet is usually an operation involving the retrieval of resources related to a site, this is not so in the dark Web.

Digital Certificates

A digital certificate proves the identity of an entity on the internet by having a trusted third party verify the entity and then provide it with a digital certificate. The certificate can be revoked in case of an issue by the issuer. A digital certificate is a requirement for SSL or secure socket layer and HTTPS that provides encrypted traffic over the Internet. This allows customers to prove the identity of a website or application they are visiting and ensure that financial transactions are made over secure channels.

Two -Factor Authentication for Payments

For credit card payments two factor authentication should be enabled. This is a method by which the user has to prove their identity to the merchant by more than one method eg. password and SMS sent to the user's phone. This ensures that the user's credentials cannot be sold and reused as the attacker would have to have both the user's authentication methods and this can prove to be difficult.

User Education

The weakest link in securing information on the web is the human element. Humans can be manipulated, coerced or tricked in to revealing sensitive information. Users need to be educated about the pitfalls of using the dark web and how to secure themselves

while using it.

Using Escrow payment providers

Using a provider like Paypal who holds funds in escrow and only releases them when there is no objection from both the customer and business can greatly increase trust in e-commerce platforms. The client will know their money is safe as the escrow payment provider has the merchants details in case of an issue. The business will also benefit by knowing that the customer is using genuine details as they have to be verified by the escrow payment provider as well.

Conclusion

'Trust' on digital platforms is a dilemma to both developing and developed economies. Anonymizing services such as Tor have been used for legal and illegal activities ranging from maintaining privacy to selling illegal goods which is mainly purchased with Bitcoin or other digital currencies. These forms of currencies are used to circumvent censorship, access blocked content, or maintain the privacy of sensitive communications or business plans. However, a range of malicious actors, from criminals to terrorists to state-sponsored spies, can also leverage cyberspace and the Dark Web which can serve as a forum for conversation, coordination, and action for illegal activities (Finklea, 2017).

A secure online platform is a must for consumer trust. Maintaining e-consumer trust poses a key challenge to digital commerce in areas of cybersecurity and privacy such as cyber breaches, threats from online payments and privacy protection. Given such a tremendous impact of potential cyber breach, it is imperative for digital commerce vendors to set cybersecurity and privacy protect as top agenda within a business's risk management framework. They should develop a holistic cybersecurity strategy to protect their customers' personal information and make sure that they develop a secure online platform.

On the other hand, digital commerce vendors should work hand in hand with e-customers to keep abreast with the latest security vulnerability, threats landscape and attack vectors. Further, collaboration between digital commerce business with their industry peers and external IT security experts may also be consider so as to ensure they keep up with the latest developments.

Digital currencies might replace traditional currencies in the future and as such businesses have to be prepared to build trust with their customers on their various platforms as to the security of using crypto-currencies or digital currencies to pay for goods and services.

References

Balasundram, M., Naranjo, L., Subramaniam, G. (2012). E-commerce best practices: How to achieve and environment of trust and security. *International Journal of Innovation, Management and Technology, 3*(4), 396-401.

Barker, D. I., & Barker, M. (2013). *Internet research illustrated.* Independence, KY: Cengage Learning.

Bartlett, J. (2014, October 5). Dark net markets: The eBay of drug dealing. *The Observer*.

Bergman, M. K. (2001). White paper: The deep web - surfacing hidden value. Retrieved from: http://quod.lib.umich. edu/j/jep/3336451.0007.104?view=text;rgn=main

Chertoff, M., & Simon, T. (2015). *The impact of the dark web on internet governance and cyber security.* London, England: Chatham House.

Delamaire, L, Abdou, H., & Pointon, J. (2009). Credit card fraud and detection: A review. *Banks and Bank Systems, 4*(2), 57-68.

Dean, M. (2014, December 18). Digital currencies fueling crime on the dark side of the internet. *Fox Business.*

Finklea, K. (2017, March 10). Dark web. *Congressional Research Service*. Retrieved from: https://fas.org/sgp/crs/misc/R44101.pdf

Gehl, R. W. (2014, October 15). Power/freedom on the Dark Web: A digital ethnography of the dark web social network. *New Media & Society.* Available online: http://nms.sagepub.com/content/early/2014/10/16/1461444814554900.full#ref-38.

Gillespie, P., Lowndes, M., Fletcher, C., Daigler, J., Dharmasthira, Y., & Shen, S. (2017, April 24). *Magic quadrant for digital commerce*. Retrieved from: https://www.gartner.com/doc/reprints?id=1−3XX4FSC&ct=170413&st=sb

Gemalto (2014). *Digital security.* Retrieved from: https://www.gemalto.com/press/pages/ge

malto-releases-findings-of-2014-breach-level-index.aspx

Paganini, P. (2012, September 17). The good and the bad of the deep web. *Security Affairs*.

PWC. (2017). *E-commerce in China – the future is already here.* Retrieved from: www.pwccn.com/en/retail-and-consumer/publications/total-retail-2017-china/total-retail-survey-2017-china-cut.pdf

UBS. (2017, October 12). *Cryptocurrencies.* Retrieved from: https://www.ubs.com/content/dam/WealthManagementAmericas/cio-impact/cryptocurrencies.pdf

Westin, K. (2014, August 22). Stolen credit cards and the black market: How the deep web underground economy works. *LinkedIn.*