SOCIAL MEDIA: THE BREEDING GROUND FOR MALICIOUS SOFTWARE

by

Jason Deshun Backers

A Capstone Project Submitted to the Faculty of

Utica College

August 2017

in Partial Fulfillment of the Requirements for the Degree of

Master of Science in Cybersecurity

Abstract

The purpose of this research was to investigate how social media has become a major breeding ground for malware. It has presented the factors that make social media a prime platform for malware breeding and propagation in addition to the risks posed by malware attacks. This research has also provided a set of recommended defense measures that may be adopted by individuals and organizations against malware-related risks. Evidently, the invaluable role played by social networks in enabling better social connectivity as well as business operations and performance makes social media irresistible to individual and enterprise users. Consequently, social networks have exponentially grown in number and adoption rates. And, malware writes have recognized these platforms as lucrative attack targets and have crafted a wide array of malicious codes to compromise unsuspecting users. Examples of malware prevalent on social media include Trojan horses, adware, spyware, viruses and worms, rootkits, ransomware, and bots and botnets. These malware programs may perpetrate fraud, threats, systems hijacking, ruined brand reputation, revenue loss, or excessive annoyance. The following are potential defense measures against malware-related risks: security technologies (e.g. antivirus software and firewalls); real-time security Web gateways; prioritization of social networking malware in IT security risk management and scoring; acceptable social media usage policy; and user awareness training/education. Keywords: Cybersecurity, Christopher Riddell, social media, social media networks/networking, social media growth, social media malware security risk, internet malware security.

Table of Contents

List of Illustrative Materials

Social Media: The Breeding Ground for Malicious Software

The purpose of this research was to investigate how social media has become a major breeding ground for malware. How have social media evolved into a prime platform for breeding malware? What are the risks related to social media technologies when exploited as a major breeding ground for malware? How can individuals and organizations using social media defend themselves against malware-related risks?

Before examining why the abovementioned phenomenon is truly a problem, it is important to start by seeking the meaning of social media. Today, social media solutions (technologies and services) have become so diverse that it is difficult to define the phrase "social media". Examples of social media solutions include Baidu, Snapchat, Facebook, WordPress, Facebook Messenger, YouTube, Pinterest, Google+, Instagram, WhatsApp, and LinkedIn among others (Hajirnis, 2015; Statistica, 2017). The actual meaning of the term may be confusing since social networking sites like Facebook, microblogs like Twitter, professional networking sites like LinkedIn, and blogs such as Techcrunch and WordPress are all generally referred to as social media technologies.

Despite the difficulties in coming up with a universal definition for social media, these tools share a number of features that may be used to better understand them. The following are some of the common features of social media (Morabito, 2016; Obar & Wildman, 2015):

- They are highly interactive as they mainly rely on Web 2.0 and similar approaches to promote user-generated content, ease of use for adoption by novel users, and compatibility;

- They emphasize personalization in that subscribers can create and manage their user accounts or profiles, which forms the basic element of implementing social interactions and connections;
- They emphasize “news feeds” and viral content such that social connections subscribers can get diverse information once they connect with others or get specific notifications from virtually every part of the world;
- Subscribers are allowed to post almost everything (like text-based messages, photo and video uploads, or hyperlinks), respond to others’ posts through likes or comments, and chat. This translates to facilitating information creation, updating and sharing;
- They are Internet-based such that interactions are all executed via online; and
- Social media firms design and maintain the social networking Websites and apps that run on PCs and mobile platforms (such as tablets and smartphones), helping subscribers interact with other individual users, groups or communities and organizations.

Therefore, social media may be simply defined as digital- or Internet-based communication technologies that enable individuals and organizations to interact or communicate with others by creating, sharing, and consuming different types of information (Hajirnis, 2015; Timm & Perez, 2010). An almost similar definition is given by Obar and Wildman (2015): computer-driven technologies that support the processes of creation, co-creation, modification, and distribution of information (such as ideas, opinions and interests) through virtual networking and community platforms.

Social media definitions drawn from common characteristics are still substantially broad. For example, blogs and social networking sites require one to have user accounts and social networks like comment and review forums or sections that make them subsets of social media but they are still distinct in nature (Leavitt, 2011). Nevertheless, the most common feature among all social media subtypes is that subscribers leverage them to distribute and manage the content (ISACA, 2010; Spencer, 2013).

Social media has attracted a huge subscriber base of younger and older generations alike (Yan, Chen, Eidenbenz, & Li, 2011). According to survey conducted by Statistica, Facebook, WhatsApp, YouTube and Facebook Messenger were the top four most popular social media platforms globally as at April 2017 based on the number of active subscribers. Each of them had surpassed the 1 billion mark in terms of active users per month. Tumblr, a blogging service had approximately 550 million monthly active users. Internet users in the excess of 2 billion have subscribed to social media and are actively using them. The popularity of social media stands to continually grow, especially with increasing mobile (device and social network) technologies adoption trends globally. The U.S., Europe, and China have the largest number of social media platforms whose membership exceeds 100 million subscribers (Statistica, 2017). These statistics are shown in Figure 1.

The diversity of social media consumers is considerably huge, for example, Facebook and Google+ mainly appeal to exchanges among relatives and friends and are driving interaction via constant status sharing, photo uploads and social gaming. Alternatively, Twitter and Tumblr are pushing rapid communication, which make them aptly referred to as microblogs (Statistica, 2017). Users can access, comment or even share news posted on social media on a global scale with unparalleled ease. This is as opposed to merely watching news on traditional broadcast media and other platforms like newspapers where little or no interactivity is supported (Kayem, 2014). Social media has also been widely used by crowd funders, political parties, religious groups, and governmental agencies to facilitate their vast online campaigns (Al-Hamami, 2014; Liaropoulos & Tsihrintzis, 2014).

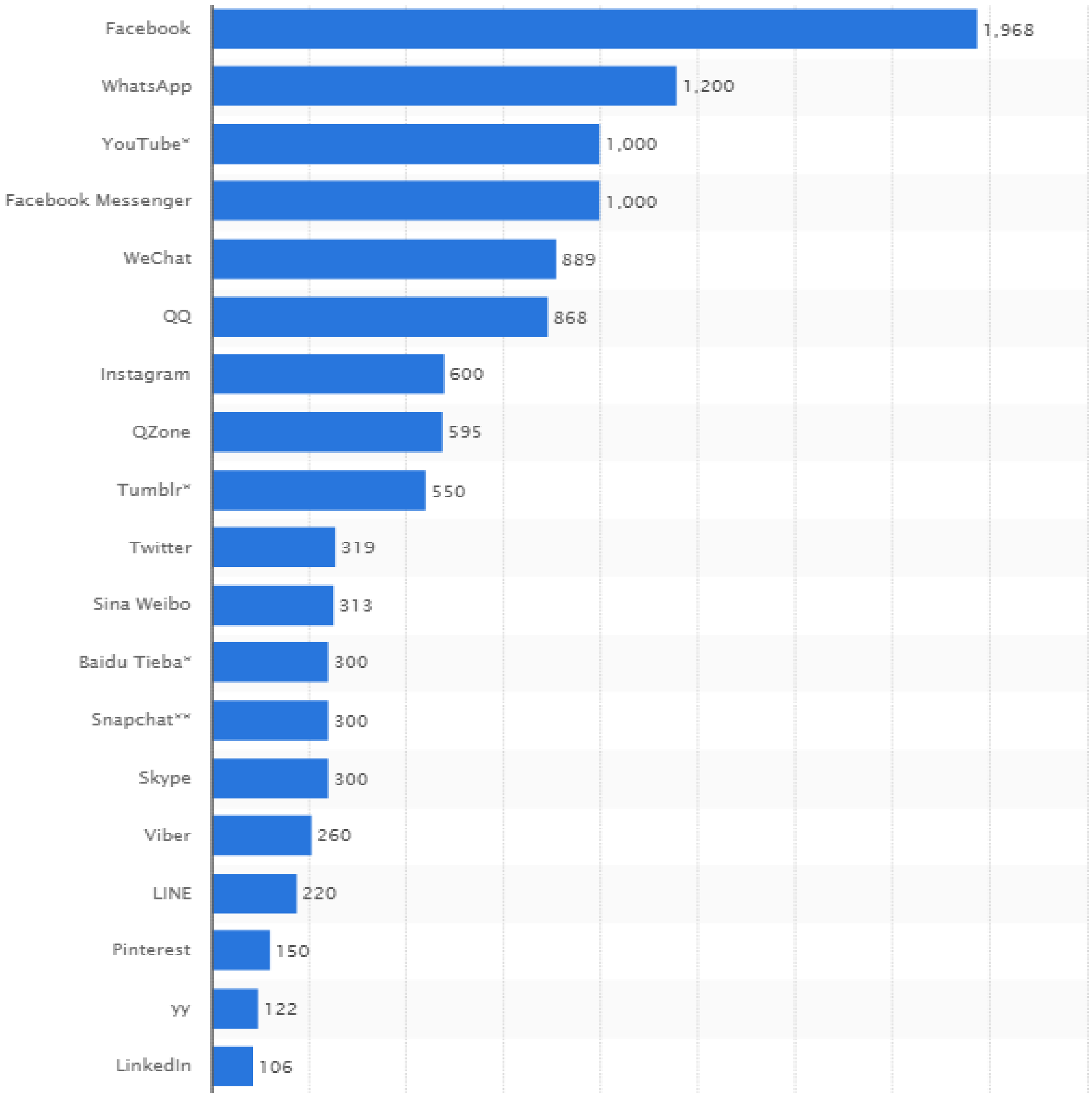

Figure 1: Most popular social media based on the number of active subscribers (in millions) as at April 2017 (Statistica, 2017).

Other than the diverse social opportunities supported by social media, they also carry valuable business potential. Social media technologies that implement time- and location-based awareness capabilities in relation to users are enabling organizations to improve their communication, discounts, e-commerce, sales promotions, market research, and loyalty initiatives (Morabito, 2016). As such, many organizations across the world have adopted social media, with 65%, 54%, 50%, and 33% of the Fortune 100 companies having active Twitter accounts, Facebook fan pages, YouTube video channels, and corporate blogs by 2010 (ISACA, 2010).

The popularity of social media also rests on being used to enhance everyday business operations and performance through the following major capabilities (Morabito, 2016; Turban, Whiteside, King, & Outland, 2017):

- Improved social networks, relationship and communication channels that promote penetration or reach and ties with corporate staff, customers, partners and the society at large;
- Search for potential employees and communicate with them using professional networks like LinkedIn;
- Online forums facilitate social marketing, which consequently drive sales revenue growth in addition to acquisition and retention of new and existing customers respectively;
- Social media likes, reviews, referrals, testimonials and brand/item followers help customer preferences that inform marketing and customer service decisions; and
- Social outlets also help monitor competition and make proactive changes to strategies and products or services.

The Internet is facing increasingly growing malware threats with approximately 300,000 new malicious codes being released every day (Brunty et al., 2014). Spammers and "phishers" – both bots and humans have identified social media as an easy and lucrative platform for bombarding people and organizations with content (Faghani & Saidi, 2009; Liaropoulos & Tsihrintzis, 2014). For example, Facebook and Twitter account owners frequently experience unsolicited interactions perpetrated through spambots that create fake or malicious accounts and use them to transmit spam content (Kaplan & Haenlein, 2010). To make matters worse, the vulnerabilities exploited do not exist in operating system flaws (Ciampa, 2012). Malicious software propagated via social media platforms range from annoying unsolicited pop ups to target individual users, and use persistent and advanced cyber-attacks on organizational social media profiles that cause severe reputational damages (Bahadur, Inasi, & De Carvalho, 2011).

Malicious programs have littered social media and it is getting worse as people tend to take little care when clicking on requests and sharing information over these platforms (Timm & Perez, 2010). Adware and spyware are particularly used by criminals to send malicious ads on social media and also to collect sensitive and confidential information without consent (Caviglione, Coccoli, & Merlo, 2013). The pervasiveness of social media and the Internet at large usually makes it extremely difficult for subscribers to know that malicious codes are continuously stealing usernames and passwords among other information that is meant to be hidden from unauthorized access (Yan et al., 2011).

Social media users are often subject to redundant adware and spyware that may compromise their devices to degrade their performance other than merely monitoring online behavior and stealing confidential information (Brunty, Miller, & Helenek, 2014). Dooley and Rooney (2017) opine that cybercriminals will continue to launch malicious apps on these highly lucrative, yet pervasive social media platforms. Hackers may be good or bad. The former category seeks to help IT vendors and consumers enhance social media security by instilling a culture of constant innovation, while the latter are into hacking mainly for malicious purposes (UcedaVelez & Morana, 2015). Malware propagation attacks are sometimes perpetrated by cybercriminals or “cyber gangs” who use sophisticated malware campaigns to severely damage or even cripple individuals’ and organizations’ social media presence (Timm & Perez, 2010).

Dunham (2008) postulates that malware attacks constitute the leading security threats facing organizations on social networking sites and the current surge in worms, ransomware, viruses, spyware, adware and other malicious programs can be to a greater extent attributed to these tools. Apparently, profile pages of social media users are one of the major breeding grounds for malware codes that may further be propagated to others through sharing of files, opening infected attachments, and clicking links (Yan et al., 2011). However, little research has been carried out to investigate the prevalence of malware threats with respect to other social media types like blogs, microblogs, and professional networking sites. Failure to be sufficiently vigilant about links and attachments shared by contacts, but most of these incidents are difficult to distinguish because the messages tend to be sent by known entities and crafted to be inoffensive (Brunty et al., 2014; Hämmerli, 2007; Johnson, 2016).

Evidently, social media has a persistent presence in almost every aspect of their subscribers’ social lives. In addition, groups and organizations are also widely using social media to support their core Internet-based social interactions and strategies, which brings the tools to the workplace (Hajirnis, 2015; ISACA, 2010; Morabito, 2016; Obar & Wildman, 2015; Timm & Perez, 2010). Ariel and Avidar (2015) argue that social media has evolved into a “big deal” mainly characterized by driving superior engagement, content co-contribution, and “social authority”. Brunty et al. (2014) assert that social media continue to drive considerable and persistent changes to the day-to-day communications between individuals, communities, and organizations. Therefore, they are one of the major technologies that have transformed the way communications and interactions are executed.

Morabito (2016) summarizes the transformative role played by social media as follows: The Internet-based technologies emphasize reliability, quality, interactivity, penetration or reach, pervasiveness or persistence, ease of use, interoperability, minimal infrastructural requirements, and speed. Therefore, these tools are driving more fun when individuals are interacting with relatives, friends and celebrities. Moreover, brands are aggressively embracing social media to meet their strategies and realize more financial success among other business benefits (ISACA, 2010). As a result, many individuals, groups and organizations are increasingly leveraging social media technologies so that they are not left behind. While social media technologies come with invaluable prospects and have captured the attention and time of a significantly growing number of subscribers, malware breeding remains one of the major problems that these transformative tools have not solved totally. Therefore, as social networks continue to grow in number and subscription rates, they have become a truly simple and lucrative ground for malware breeding.

Literature Review

This section presents a comprehensive review of literature relevant to the overall research topic, purpose statement, and research questions. Basically, it is an evaluation of past research works conducted in the field of social media and cybersecurity, while paying close attention to malware breeding and propagation. Moreover, it evaluates literature on malware security risks in addition to potential avoidance and mitigation techniques. This has helped gain a sound impression and/or sense about crucial aspects and relationships between various concepts in relation to the topic towards identifying ideas worth further considerations. For this literature review, previous findings are structured per each of the already formulated research questions.

Social Media as a Prime Platform for Breeding Malware

Human history has never before had a population that is aggressively adopting technology advances like in the 21st C. In the Internet era, social media remains one of the most quickly and widely embraced technologies worldwide with consumers seeking valuable social, economic, religious and political prospects (Tipton & Nozaki, 2012). Many social media applications have been developed over years, leading to a consistent growth in their size (Kayem, 2014). In addition, consumers embrace them considerably fast. A case in point is Facebook, which received statistically significant adoption rates within the first four years after its release by surpassing 100 million subscribers (Abraham & Chengalur-Smith, 2010).

With networks such as Facebook and YouTube surpassing the 1 billion mark in active user base as of April 2017 and others such as Twitter and Skype recording about 300 million, it is apparent that the global social media network is continually expanding (Statistica, 2017). Social media networks are increasingly becoming bigger; thus they are good ventures for attackers out to make a killing by exploiting big and lucrative targets (Waters, 2011). Therefore, Facebook, LinkedIn, MySpace, Bebo, Instagram and other general public social networks present malware attackers with a huge payoff among other opportunities. Brunty et al. (2014) assert that social media sites are natural targets for malware because of their large membership and global popularity.

The growing popularity of social media is mainly because they assure the following major capabilities that gives them an edge over traditional media: instant global reach; support for multipurpose services (like access to news and sharing of photos); accessibility to the public; no or insignificant cost; minimal specialized hardware and software requirements; ease of use (no specialized skills required to operate them); and greater profile personalization potential

(Gao, Hu, Huang, Wang, & Chen, 2011; Hajirnis, 2015; Kayem, 2014; Morabito, 2016). However, the popularity of Facebook and other social media has been faulted by critics who argue that the number of registered users may not measure the actual active usage of these tools (Abraham & Chengalur-Smith, 2010; Morabito, 2016). That aside, hundreds of thousands of social media profiles are created every day in search of benefits associated with these tools. Social media represents a pool of crucial information about individuals, groups and communities, and organizations (Abouzakhar, 2015).

To promote openness, social media are purposely designed to expose as much confidential and saleable information about subscribers as possible (Waters, 2011). At the same time, cybercriminals have jumped into this much-hyped journey with subscribers to breed and propagate their malware despite several attempts to address existing and potential vulnerabilities and threats (Caviglione et al., 2013; Filiol, & Erra, 2012). On these networks, many people forget about the impending security threats and fail to observe secure practices. Past works (Gao et al., 2011; Harkins, 2012; Management Association, Information Resources, 2015; Yan et al., 2011) have shown that malware attacks succeed on social media because people are ready and quick to click on messages and links regardless of the source. The implication is clear – users are largely unaware about malware being attached to social media and that they stand to fall victims to these scams for attackers' selfish ends.

Majority of social media users are yet to beware in relation to impending malware threats facing them when engaging the tools. In the middle of an epidemic, malware, people are busy and comfortably sharing their ideas, feelings, and current locations, while simultaneously liking others' posts and comments (Hekkala, Väyrynen, & Wiander, 2012). The situation might easily get worse in the future as criminals make codes and tricks more advanced for the average user and the public to discern (Sanzgiri et al., 2013). Even worse is the fact that social media networks are easily accessible and extensively used, which makes them irresistible to malware criminals (Abraham & Chengalur-Smith, 2010).

Explosion of Malware Security Threats to Social Media Networks

Brunty et al. (2014) point out that the lineup of malware threats facing social media networks worldwide is mainly a common one, and it includes Trojans, adware, spyware, viruses and worms, rootkits, ransomware, and bots and botnets. Collectively, these familiar techniques tend to characterize malware attacks that may be successfully executed by leveraging social media (He, 2013).

The Koobface worm is identified as perfect example of attacks targeting social media and spreading by sending messages from victims' accounts to friends, with Facebook, MySpace, Twitter, Bebo, and Friendster being the largely exploited distribution channels (Abouzakhar, 2015; Timm & Perez, 2010). Koobface is designed to systematically direct recipients to a third-part app from where it prompts them to download a specific file as the app's update. Devices are infected with the worm when the file is downloaded. Moreover, attackers may take over the search engine installed on the victim's system and download contaminated files (Baltazar et al., 2009; Filiol, & Erra, 2012). Once a system (like a machine or Web browser) is infected, malware launches further attacks such as DoS, data theft, unwanted data encryption, or annoyance among others. As more protection and prevention controls continue to emerge, the attackers respond by changing the attack avenues for breeding and propagation of these malicious programs (Brunty et al., 2014; Timm & Perez, 2010).

Today, attackers are trying to gain access to billions of people sharing a social network with limitless trust. And, diverse malware types are being bred and delivered over these networks on a day-to-day basis (Athanasopoulos et al., 2008; Thomas & Nicol, 2010). This implies that creating social media presence brings consumers into the “bull’s eye” of cybercriminals and the risk of malware infections and/or attacks. Botnets may illegitimately use social media sites (like Twitter and Tumblr) as their command and control channel (CNC) and users as bots. Massive traffic helps hide the CNC of botnets and it makes it challenging to determine and trace the botnet attackers (Batten, Li, Niu, & Warren, 2014; Timm & Perez, 2010).

Social Media as a Malware Attack Platform

Social media networks and services were not designed with sufficient security considerations. Instead, they evolved and grew in popularity around an emphasis on ease of use, communication and engagement. This has been cited as the main factor that makes these platforms inherently at threat of malware attacks and mischief (Sanzgiri, Hughes, & Upadhyaya, 2013; Waters, 2011). And, malware attack criminals are coming up with creative and innovative tools and techniques to exploit social media at every possible level (Abraham & Chengalur-Smith, 2010). Dunham (2008) explores the existence of security vulnerabilities in social media technologies themselves due to design flaws that may be exploited to propagate malware codes and conceal their actions. While Trojan horses and worms often spread very fast even on other platforms like USBs, social media has helped malware writers reach their targets where there is more weakness with more ease and speed (Sanzgiri et al., 2013).

Cross-site scripting (XSS) is a popular type of attack that entails forcing a victim’s browser to execute a code. Researchers have indicated that approximately “80% of Web applications” are vulnerable to XSS attacks because they allow tags as inputs in their input forms. This implies increased threat because criminals can inject malware into the Web applications through the tags (Faghani & Saidi, 2009).

The channel for XSS attack is the vulnerable social media site, which is exploited by criminals to attack users (Green, 2015). When an attacker finds an XSS exploit in one of the popular social networking sites, the number of potential victims could be in excess of millions (Timm & Perez, 2010).

The first widely known XSS-related malware was “Samy”, a worm that exploited an XSS weakness in MySpace.com’s user profile page template. The worm’s payload is designed to force the victim’s browser to accept “Samy” as a friend when a verified MySpace.com’s user viewed the fake profile of “Samy”. In addition, it forced the browser to include the tag to the user’s personal profile, and modify the compromised profile with the malware’s copy. The worm infected over 1 million user profiles within a single day since every user who visited a victim contracted the malware, and so on. Other than MySpace, Twitter, Gaia and hi5 have also faced several active XSS worms like Code Red I, Code Red II, and Slammer (Al-Hamami, 2014; Faghani & Saidi, 2009; Timm & Perez, 2010).

Third-Party Apps Hosted on Social Media.

Genuine third-party apps may come with security weaknesses that cybercriminals exploit to promote malware via social networks. Most social media networks allow addition or installation of these third-party apps to support services such as gaming and photo sharing. These apps may have access to personal profile accounts and information. As such, criminals may exploit potential vulnerabilities found on these apps to steal personal information using spyware and related malware programs (Al-Hamami, 2014; Waters, 2011).

There are rogue applications that are built by attackers to compromise social media subscribers and perform harmful activities. Like-jacking, click-jacking, and share-jacking are examples of malware attacks (more specifically worms) to social media.

They trick unsuspecting users into liking an item, using a feature, and sharing something on their profiles without their consent. The attack starts off from an unsolicited request where one is offered a chance to get access to something. Upon accepting the request, a malicious script from a different domain loads silently. Eventually, the victim's profile page shares content and links users to the malicious external domain. On clicking the malicious link, users are likely to fall victims (Abraham & Chengalur-Smith, 2010; Batten et al., 2014). Therefore, the attackers are able to virally spread the malware threat to as many users as possible using such third-party app tricks. Typically, these types of malware attacks make victims believe that they are accessing notifications from apps shared with friends. However, the buttons (like "Next") to complete a number of steps are in reality implementing "like", "share" and such functions. This promotes the propagation of such worms (Abraham & Chengalur-Smith, 2010).

There are worms that provide a link, which takes users to a different page when clicked as the initial malware attack technique (Brunty et al., 2014). Brunty et al. (2014) further claim that social media remains a big target for such clickjacking attacks. On the new page, one may be required to download and install a software version so as to be able to continue. It is here that most of the people who are not mindful or aware about social engineering are infected on they click the download or install buttons (Thomas & Nicol, 2010). Hekkala et al. (2012) opine that some click-jacks are crafted to redirect victims to sites contaminated with malware from where their personal information and identity is put at risk.

The popularity of these malware programs has not been explicitly ascertained by research, but Brunty et al. (2014) claim that cybercriminals frequently attempt to spread malware using clickjacking, drive-by downloads, and "malvertisements" to install malicious apps, create fake user or corporate profiles, or send corrupt messages. Actual attack statistics cannot be readily accessed since social media network operators may also not be willing to scare their users by disclosing the prevalence of these threats and successful infections (Brunty et al., 2014). Organizations on social media risk persistent and sophisticated malware campaigns carried out by criminals out to demand for ransom or steal confidential data (Management Association, Information Resources, 2015). Therefore, other than annoying adware, social medial is a prime platform for launching distressing ransomware and viruses.

The Viral and Pervasive Nature of Social Media

Timm and Perez (2010) argue that users place excessive trust in social media networks and affiliated third-party apps, which make it simpler for criminals to masquerade as legit third-party players and propagate unwanted and malicious codes. The problem is further complicated by the fact that social media networks are inherently viral (Yan et al., 2011). What can be deduced from the two challenges is that these networks are vast breeding grounds for malicious software. A lot of malware, including spyware, ransomware, spyware, viruses, Trojan horses, and bots are rampant on social media. The fact that social media networks are intrinsically viral makes it substantially easy for malware writers to spread huge loads of malware (Thomas & Nicol, 2010). Nevertheless, most organizations are leaving an exploitable spot by failing to incorporate social media vulnerability and threats into their risk identification, scoring and management (Zurkus, 2016).

The Dynamic Nature of Web 2.0

Web 2.0 is the basis behind social media networks of today (Timm & Perez, 2010). The dynamism introduced by Web 2.0 has made it possible for social media networks to allow subscribers to generate as much content as they can, upload it on these platforms, and perform a myriad of tasks on the social Web. In contrary, the conventional static Web 1.0 could only allow skilled persons to create content and it was challenging to modify it once uploaded (Sophia van Zyl, 2009). The major capabilities brought about by Web 2.0 may be summarized as a move from home pages and personal websites to blogging, "page views" to "cost per click", publishing to participation, reading to writing, companies to communities, owning to sharing, and directories to tagging (Timm & Perez, 2010).

Social networks have a global appeal as the human desire of online communication continues to thrive via Web 2.0 applications. Social media systems have led to a rich arena of collaborative and information sharing technologies for the Web that have transformed hosted service effectiveness and efficiencies. Consequently, a plethora of social networking sites, blogs, professional networking sites, shared video sites and other Web 2.0 applications have emerged (Timm & Perez, 2010). As a result, human-Web interactions have taken shape and the content flowing through the dynamic Web applications is increasingly gaining value as human interactions enrich it.

All the good intentions aside, cybercriminals have seen this as an opportunity to launch low- to serious-magnitude malware attacks. After all, social networks are designed to allow users to perform a lot of tasks related to information sharing and interactions that carry immense capital (Baltazar, Costoya, & Flores, 2009; Sophia van Zyl, 2009. In addition, both social media users and criminals take part in spreading malicious codes on social media effortlessly as they generate and share endless content (Baltazar, Costoya, & Flores, 2009). According to Faghani and Saidi (2009), social media networks provide a means of bringing together millions of users who are heavily connected, which aids in rapid distribution of malware across the globe.

Malware writers also exploit the excessive trust among social media users to spread their malware (Faghani & Saidi, 2009).

Social Media Risks in Relation to Malware Breeding and Propagation

Studies have shown that increased social media usage is a recipe for increased malware infections (Faghani & Saidi, 2009; Hekkala et al., 2012). The malware threats on social media have already evolved beyond mere viruses and worms into more plaguing malicious programs, especially stealthy ransomware that download into user devices and encrypt all files. Ransomware are especially disastrous because users are not assured that their files will be accessible upon settling the demanded ransom, which is mainly in real monetary or bit coin form. Ransomware not only corrupt data and demand for ransom, but it can also allow attackers to hijack user devices (Bahadur et al., 2011). Therefore, ransomware entails a high-level security threat and social media may be used to transmit Trojan viruses that facilitate replication.

Ransomware victims are threatened to pay a specified fee to have their invaluable locked hard drives and encrypted files unlocked. Alternatively, criminals may threaten the victims that their personal data will be published to the public if the demanded fee is not paid within a specified timeframe (Thomas & Nicol, 2010).

Scareware and rogueware are types of malware that trick Internet users into believing they may facilitate removal of some form of malware infection. Pop ups on social media may be used to provide links to this fake malware clean up software, which may allow for serious malware injection (UcedaVelez & Morana, 2015). Average users on social media are likely to easily fall victims to these Trojan-based scams as they disguise themselves as legit files to increase the probability of being opened or downloaded (Yan et al., 2011). Attackers may use botnets to advertise computer protection software and infect the unsuspecting victim’s system upon clicking the provided link. Then, the botnet prompts specific attack commands that may trigger ransom and other extortion attacks (Timm & Perez, 2010).

Data Theft/Leakage and Systems Downtime

Worms and Trojan horses have been associated with disastrous damages to data and computer networks. For example, the malware could delete, modify, copy, and steal data or disrupt normal network activity. In the context of social media networks, Trojan horse covers up malware such as worms to make it appear like an ordinary and harmless file. This tricks social media users into allowed malicious files into their devices (Picazo-Vela, Gutiérrez-Martínez, & Luna-Reyes, 2012). The Internet remains an invaluable landscape for Trojan viruses and worms, and so is social media. Backdoor Trojans use a computer as a backdoor to allow the cybercriminal to gain its access and control. Then, this malware may stealthily steal data, manipulate other machines, or even inject more malicious codes onto devices (Joe & Ramakrishnan, 2014).

Joe and Ramakrishnan (2014) note that social media users are exposed to harmful downloader Trojans that may be injected onto their devices from where they risk continuously downloading additional malware. The level of risk may range from annoying behaviors to distressing incidents of data theft and system crashes. Other risks include the victim being denied access or control to the machine (Abraham & Chengalur-Smith, 2010). To make matters worse, worms spread very fast through autonomous replication, while infecting devices and deleting or modifying data (Labuschagne & Veerasamy, 2013).

Harkins (2012) notes that botnets that trick unsuspecting users into downloading applications such as fake security software may be used to launch a number of attacks, including DoS and DDoS, spamming, sniffing, and key logging. Therefore, these malware attacks that are rife on social media may eventually lead to compromised data loss and systems interruption. Trojan horses, rootkits and keyloggers are some of the common concealment malware programs that perform undesirable actions, including unauthorized data and systems access, alteration of processes and files, and theft of sensitive data like passwords and bank account details (UcedaVelez & Morana, 2015). Therefore, malware emanating from a social media presence may infect enterprise systems, causing unwanted data leakage or leakage and downtime.

“Owned” Systems – Zombies and Puppets.

Bots are malicious applications that execute automated activities on compromised user devices, especially attacking a chain of other machines using an infected computer – “zombie” (Dunham, 2008). Indeed, research of prevalence bots and botnets on social media is significant and there are serious documented cases of such types of attacks originating from social media, for example, the Koobface. Timm and Perez (2010) opine that bots may be bred on social media and used to inject adware and spyware onto other devices. From the perspective of social media and malware, spyware is designed to hide on social media or user devices and then silently monitor everything or steal data such as usernames and passwords. Furthermore, it can monitor Web activity as the basis for launching further malicious attacks (Joe & Ramakrishnan, 2014).

Criminals also target social media websites with browser hijacking malware. These are codes that maliciously redirect a browser from one site to another. While browser hijacking mainly seeks to display advertisements, it may also generate unwanted visits to specific websites that download some malicious software onto users’ devices (Abraham & Chengalur-Smith, 2010). Timm and Perez (2010) associate puppetnets and botnets with increased social media attacks. While the two threats are mistaken to be similar, they differ in that the former targets Web browsers while the latter seeks to compromise PCs and sometimes IRC servers. Puppetnets allows the attacker to take control of the victim’s Web browser when the user visits a contaminated site or page and logs on to it. The user is turned into a “puppet” while on the malicious site/page because the attacker can be simultaneously executing malicious activities without the knowledge of the victim by running an attack code in the browser (Timm & Perez, 2010).

Ciampa (2012) postulates that puppetnets compromise browsers and launches further attacks against the victims’ systems. In addition, they conceal their malicious activities by adopting background operations. Unexpected slow connections are the main indicator that something bad is taking place, which makes the victim almost totally unaware of an ongoing or impending attack. Then, the puppetnet is destroyed with a lot more ease than it is the case for botnets (Athanasopoulos et al., 2008; Timm & Perez, 2010).

In the context of social media, an attacker may build an app like a game with a malicious code. Then, the criminal would create a fake account, befriend a large number of people, and send them the game. This way, the malware would be propagated to as many users as possible and their browsers may be eventually hijacked (Timm & Perez, 2010). As such, some malicious programs bred on social media are likely to hijack user devices and Web browsers. Attackers could use hijacked systems to launch further information security breaches like spamming, data theft, file and hard drive encryption, and systems and network disruption.

Damaged Brand Reputation and Revenue Loss

Organizations are establishing strong social media presence as part of business strategy to make their brands more successful. It opens many opportunities for business growth and connection with customers, staff and partners. As the same time, this platform opens room for a lot of activities, most of which take place in a highly pervasive manner (Green, 2015). Social networking malware security controls, policies and procedures are struggling to handle the exponentially growing number and types of malware threats and attacks. Consequently, malware spread via social media networks as well as spoofed profiles and pages attract information breach risk for organizations. A study conducted by security professionals at Panda showed that almost 33% of small businesses have suffered some form of social media malware (Morabito, 2016). While this is widely motivated by the popularity of Facebook, criminals are exploiting social media platforms as their main domain for malware distribution.

In particular, approximately 78% of businesses leverage social networks to advertise their brand and products. Approximately 52% of company employees confirmed that they had seen an increase in malware due to staff use of these networks (Morabito, 2016). With surging malware threats on social media, organizations stand to have their login credentials stolen using malicious programs such as spyware without being detected. Criminals may then use the opportunity to publish unwanted content or send spam messages to people using the hijacked account before it is disabled or recovered. Moreover, malicious people may spread misleading information over the compromised brand account (Chaudhry, 2017). Consequently, compromised companies may suffer serious brand reputation.

Social engineering and botnet malware criminals are increasingly targeting social media sites as these networks continue being flocked by millions of subscribers. The Koobface botnet has particularly been designed to leverage "zombies" to automatically generate fake social media accounts, befriend target victims, and spread malware spam on Twitter and Facebook (Baltazar et al., 2009). Baltazar et al. (2009) examines the zombie infrastructure for Koobface in addition to the malware's activity on social media. The botnet generated several fraudulent social network site accounts and sent malicious links to approximately 213,000 users, attracting more than

157,000 clicks (Baltazar et al., 2009). The Koobface worm infects a victim's computer and sends spammed comments to the profiles of friends who are likely to believe in the legitimacy of those messages as they appear to originate from people or brands they know. The spam may also carry some malware with it, implying further imminent problems (Waters, 2011).

Waters (2011) states that the accounts generated by zombies look official and include professional designs to make it difficult for befriended victims to tell that criminals were running them. It is people who tend to fail to recognize potential malware security risks and act accordingly, allowing perpetrators to take over and launch their dangerous activities. Criminals are targeting social media accounts that are mainly left unmonitored for long and imitate them to send offensive messages and spread malware programs such viruses and worms to friends and followers (Thuraisingham et al., 2016; Waters, 2011). A compromised corporate account may continuously be used to send fans and followers spammed content, which may lead to loss of brand confidence, reputation, or trust (Morabito, 2016).

As previously stated, the proliferation of social media has led to a surge in malware security risks for scores of organizations (Morabito, 2016). If a malware breaches information security due to the day-to-day employees' social networking activities, then the attacked organization risk its reputation or credibility being ruined (Spencer, 2013). Consequently, it is possible to as well lose existing customers and suffer plummeting sales revenue. Revenue loss may also arise from business disruption in the event that a malware attack crashes a critical information system or causes a prolonged outage. In addition, the costs of repairs to infected systems in addition to legal liabilities could drive up expenses and decrease profit margins. The cost of a massive data/information breach could exceed £100 million. Data loss can cause a disastrous financial impact on a company, which when combined with business disruption, damaged consumer confidence, recovery costs (related to cleaning systems and data), and sales revenue drop could send it into unexpected bankruptcy (Morabito, 2016).

Excessive Annoyance

Not all malicious software is inherently destructive. Nevertheless, users stand to face exceedingly irritating such as being bombardment with excessive pop-up ads. Adware is especially associated with displaying unsolicited advertisements on user profiles through pop-ups. Some adware codes are designed to redirect from social media to a particular site (Joe & Ramakrishnan, 2014). Thomas and Nicol (2010) postulate that adware may not necessarily cause direct impacts to users' devices, but it can also introduce spyware. Viruses and other malware found on social media can make infected computers, tablets and smartphones crash or run slowly by consuming excessive memory through unwanted processes (Obar & Wildman, 2015). At the same time, social media users stand to lose sensitive data unknowingly as they carry out their usual activities (Faghani & Saidi, 2009).

Defense Measures Against Social Media and Malware-Related Risks

According to Yan et al. (2011), firewalls and anti-malware programs are the obvious protection measures from malware propagated via social media. Therefore, individuals and organizations should emphasize running up-to-date and proven antivirus software and firewalls at end-point and network levels to reduce or mitigate social media malware threats. This creates a social media engagement platform that is secure from potential malware attacks. Anti-malware security programs should be implemented on PCs and mobile devices to facilitate continuous scanning for suspiciously malicious links and apps when on social media (Furnell & Clarke, 2007).

Zurkus (2016) proposes adoption of proven Internet security software to protect social media users against surging malware threats. Considering that users can easily contract serious malicious codes by clicking on or visiting compromised pop-ups or sites respectively, an effective Internet security software becomes a vital necessity for intercepting concealed threats on social media platforms.

Thuraisingham et al. (2016) argue that proxy servers and/or Web filtering tools may be utilized to help block executables as they are closely associated with malware. Content filters may also be used to limit or restrict social media access within the enterprise network (ISACA, 2010). Firewalls are crucial tools for blocking incoming and outgoing connections to a set of unnecessary ports and services (Harkins, 2012). According to Timm and Perez (2010), Web filters perform "input filtering blacklists" to prevent or mitigate XSS exploits. However, Al-Hamami (2014) argues that filtering blacklists are not as effective as they are perceived to be; attackers can successfully circumvent them and upload their malicious codes.

Real-Time Security Web Gateways

Zurkus (2016) states that the required security controls should go beyond anti-virus programs and firewalls that are based on rigid policy and signature techniques since they are inadequate. However, research shows they are essential Internet security technologies (Zurkus, 2016). Zurkus (2016) proposes adoption of securely configured Web gateways together with firewalls and anti-malware programs as the best approach to protection against social media malware threats. By analyzing links based on its appearance as opposed to looking for a known or recognizable payload or signature, such tools address the threat of new links posted on social media to redirect users to websites that download malware through disguised scripts (Joe & Ramakrishnan, 2014). With the mobility supported by social media technologies, these real-time

Internet security tools enable on-the-fly content analysis. Therefore, social media users are secured from malware at data creation, modification, and consumption points (Zurkus, 2016).

Prioritization of Social Media Malware in IT Security Risk Assessment and Scoring

Small to large organizations have introduced social media usage into the workplace to achieve strategic business goals in the areas of PR, customer service, marketing, relationships and loyalty initiatives, and partnerships (Picazo-Vela et al., 2012; Sophia van Zyl, 2009). Therefore, organizations are at a serious malware security threat and appropriate controls need to be implemented to prevent or mitigate the risk. According to Picazo-Vela et al. (2012), organizations should reconsider their IT security risk assessment scoring systems and prioritize social media as it has evolved into to top ground for the current and future cybersecurity threats. Apparently, social media usage has increased and so has malware over the recent years. However, insignificant research efforts have been directed at the correlation between growth in social media popularity and the surge in malware. What is widely agreed is that: when one interacts with a social network like Facebook or LinkedIn, there are chances of facing social media tricks seeking to propagate malware and cause infection (Hämmerli, 2007).

There is insignificant to no end-to-end visibility into the vast social media platforms as they are external to the enterprise network perimeter. When challenged visibility is coupled with unparalleled pervasiveness, social media have become one of the most dynamic and uncontrollable risks to individuals and organizations (Faghani & Saidi, 2009). This is despite the fact that social media has become a major corporate communication tool, and that criminals are aggressively trying to exploit any weaknesses. Indeed, social media sites are gateways of malware that sit outside the end-point security (Zurkus, 2016).

As such, prioritizing such risk using Common Vulnerability Scoring System (CVSS) score solely would not bring the desired results. It is important to use a combination of factors as sub-scores to incorporate the concepts of context, content feeds, and trend analysis to deliver effective malware risk assessment and prioritization (Zurkus, 2016). Therefore, organizations ought to assess the likelihood of contracting malware from employees' social media activities. Moreover, the probable attack impact severity and risk levels to the company should be evaluated towards coming up with sufficiently effective controls or defense measures (Picazo-Vela et al., 2012). With a clear understanding of malware threats in relation to social media use, it is possible to channel resources into the right countermeasures. Consequently, resource wastage and complacency issues are minimized.

Acceptable Social Media Usage Policy

A policy to compliment deployed controls should be formulated to make sure that employees are well-informed about the accountable, secure, and acceptable social media use at work. Communication of social media policy should be prioritized to help employees understand its existence and applicable requirements (Picazo-Vela et al., 2012). Nevertheless, what social media policy requirements must be included for optimal effectiveness? Brunty et al. (2014) identifies the following practices as the most acceptable social media usage at work: networking with colleagues and friends within and outside the organization; and texting and emailing. On the contrary, the least acceptable practice at work from the perspective of malware security is downloading applications from social media networks as it can lead to injection and spreading of malicious codes (Sophia van Zyl, 2009).

Requirements define the dos and don’ts in relation to different parties (such as senior executives, business managers, IT managers, legal and policy personnel and staff) as well as social media channels. In addition, social media policy should provide best practices, procedures and guidelines on plans to secure social media networks and run training initiatives (Bahadur et al., 2011). Therefore, the policy represents some form of a strategy of limiting social media access and use. However, social media is almost inseparable from humans’ social life and business strategy, thus restrictions should be pursued with care to ensure that inherent benefits are realized to all parties. It is for this reason that Kayem (2014) proposes that organizations should strike the right balance between limiting social media access and malware security considerations. It is recommended that the personnel involved in social media engagement on behalf of their brand should have undergone training in the implemented policy requirements. In addition, the personnel should be well versed with controls deployed to protect their company (Bahadur et al., 2011).

Social media requirements ought to be explicitly communicated to employees for maximum effectiveness of the policy. This can be attributed to the fact that use of social media for personal and business functions equally increases the likelihood of malware threats, and care must be taken to reduce associated risks (Yan et al., 2011). Malware risk remains even with presence of a well-communicated policy or banning social media networks if employees fail to comply with specified requirements. As such, the policy should be enforced accordingly to make sure employees face disciplinary actions if they breach any of the requirements (Thomas & Nicol, 2010). Bahadur et al. (2011) assert that other than communications and training, proper social media use policy requirements must be enforced. However, research shows that poor management and governance in addition to inadequacy of resources to check compliance are the major causes of widespread failure to enforce acceptable social media uses (ISACA, 2010).

User Awareness Training/Education

Social media subscribers should be treated as the first “line of defense” against malware propagated on these Internet-based networks. However, attackers have found an easier platform for spreading malware hidden as spam links and content because of user unawareness (Gao et al., 2010). Therefore, there are skill gaps that need to be closed through well-planned training and awareness initiatives towards arming individuals and organizations against malware codes that are prevalent on social media networks. Luckily, some network operators like Facebook run security and policy pages from where users can learn about the latest security threats among other skills essential to secure online communications and other engagements (Picazo-Vela et al., 2012). The move may make people and organizations more careful with social media malware security and motivate them to continually monitor their accounts for malware and act accordingly.

Thuraisingham et al. (2016) argue that training and awareness reduces the likelihood of human error; users are enabled to avoid accidental interactions with suspiciously malicious programs like pop up adware and spyware forms. Users should be provided with means through which they can detect potential malicious tools and tricks on social media, which Gao et al. (2010) argues such a move may help target victims avoid malware-related threats. Therefore, organizations leveraging social media to improve their efficiencies across different fronts have social media training at their disposal to increase the successfulness of Internet-based malware protection.

Sharing malware-infected content via social media networks also increases the likelihood of facing malware attacks that would be otherwise avoided if users are empowered to engage in a security-conscious manner. Therefore, social media policy for promoting and enforcing acceptable use should be reinforced with comprehensive training to bring all potential gaps and issues in social media malware security to the limelight (Bahadur et al., 2011). Therefore, it is important to walk social media users through what they should and shouldn't engage in and how to ensure continued compliance with implemented policies.

One of the most basic skills is being able to recognize unsafe links and behaviors on social media. In addition, subscribers ought to be encouraged to report potentially malicious concerns to social network operators and their employers to ensure preventive or corrective measures are taken in a timely manner (Furnell & Clarke, 2007). Policy training should be treated as a major enabler of avoiding full-scale and persistent malware attacks. In case of compromise, it is also the best approach to quick recovery within minimal time and damages as it provides guidelines and procedures necessary to bring address different problems (Bahadur et al., 2011).

Training and awareness programs are also associated with increased knowhow with respect to understanding what to pay attention to as far as malware threats on social media are concerned (Timm & Perez, 2010). Investing in training will go a long way in helping users put their guards very high and bring social media within sufficient organizational control. For example, people will be quite careful when engaging with third-party apps. Users will be motivated to be extra careful when clicking on unsolicited links, content and sites, and avoid suspicious requests and offers provided they understand the risks. Raising awareness influences behavioral changes, which in turn heighten security.

For example, social engineering tricks and attacks (such as spam, phishing and fake websites) that precede and conceal potential malware injection incidents will be easy to detect and avoid. Attackers basically propagate bots, puppetnets, Trojans and other malware and users can discover potential infections through factors such as noticeable slowdown in system response time and internet connection speeds (Faghani & Saidi, 2009; Gao et al., 2010).

OS and browser security updates and patches should also be emphasized among users to avoid zero-day exploits that criminals are accustomed to (Abraham & Chengalur-Smith, 2010). Moreover, the anti-malware software deployed at network and host levels should also be kept up-to-date (Thomas & Nicol, 2010). For puppetnets and other malware that occur in Web browsers, users should be trained on additional mitigation techniques like disabling JavaScript and block pop-ups in addition to limiting the number of allowed connections. While these security controls appear to be extremely simple, they may help in preventing become a "puppet" when puppetnets attack and in avoiding further malware attacks (Athanasopoulos et al., 2008).

Discussion of the Findings

The purpose of this research was to investigate how social media has become a major breeding ground for malware. How have social media evolved into a prime platform for breeding malware? What are the risks related to social media technologies when exploited as a major breeding ground for malware? How can individuals and organizations using social media defend themselves against malware-related risks?

The Meaning of "Social Media"

What should be regarded as "social media"? This research has shown that "social media" is an umbrella phrase that basically entails the creation and distribution of different forms of content (text, video, audio, images and others) through Internet-mediated technologies. Social media differs from traditional networking in that the former provides higher levels of interaction, engagement, and global accessibility to consumers compared to the latter (Gao et al., 2011; ISACA, 2010; Morabito, 2016; Obar & Wildman, 2015). As such, it allows consumers to post something, comment, discuss, and receive and disseminate content.

Use of modern social media tools and services (such as Baidu, Snapchat, Facebook, WordPress, Flickr, Facebook Messenger, YouTube, Pinterest, Google+, Instagram, WhatsApp, LinkedIn, QZone, Viber, yy, Skype, and Sina Weibo) has enabled highly effective and efficient communications in real-time for any user irrespective of geographical location. The most common link across all social media types is that it is the users who supply and manage the content by leveraging the technologies and platforms run by social media operators (ISACA, 2010). Social media leverages the power of Web 2.0 to facilitate blogging, participation and collaboration, writing, active communities, sharing, and tagging among other capabilities relevant to information sharing and dissemination (Timm & Perez, 2010).

Value of Social Media

Social media tools support information creation and dissemination. Here, information refers to any expression – ideas, feelings, career opportunities and interests, news, schedules, and others. As such, they allow like-minded persons, groups and communities to connect, collaborate, and engage with others (Obar & Wildman, 2015). However, each form of social media is designed around an idea: blogs (e.g. WordPress for creating blogs); microblogs (e.g.

Twitter for breaking news); video and audio sharing (e.g. YouTube and Flickr for entertainment and news delivery); professional networking (e.g. LinkedIn for job searches, skills/knowledge transfer and business relationships); and social networking sites (e.g. MySpace and Facebook for making new friends and connecting with them). As such, social media tools bolter social connectivity among users enabling them to network with their colleagues, friends, relatives and others in real-time and without any geographical constraints. In addition, compared to conventional media services such as TV broadcasting, news delivered via social media allow users to respond to them through comments.

Social media technologies have also been introduced into the enterprise almost as a rule because of their exceptional value creation in the areas of brand recognition, sales and marketing, customer service, revenue generation, internal and external relationships, employee recruitment, revenue growth, and innovation (ISACA, 2010; Morabito, 2016). Other than the ease of access and usability benefits, social media networks are purposely designed to expose as much personal and saleable information about users as possible. Therefore, organizations have recognized these tools as mandatory for adoption to meet their strategic goals (Waters, 2011). However, an appropriate social media strategy is required to assure ROI by avoiding and/or mitigating negative impacts, such as information security breaches, ruined reputation, recovery costs, loss of customers, and legal liabilities (ISACA, 2010; Labuschagne & Veerasamy, 2013).

Social Media and Malware Breeding

Social media tools come with unparalleled levels of ease of use, reliability, interactivity, reach, persistence, interoperability, communication speed, and affordability and accessibility.

These capabilities have made social media a powerful and irresistible force for social connectivity as well as for organizations to reach, engage, and attract stakeholders such as employees, customers and partners (Labuschagne & Veerasamy, 2013; Morabito; 2016).

And, as millions of people flock Internet-driven social networks that are equally growing in size, criminals have identified these platforms as attractive and lucrative targets for their malicious codes (Abraham & Chengalur-Smith, 2010; Brunty et al., 2014; Thomas & Nicol, 2010). Labuschagne and Veerasamy (2013) postulate that even a 1% success rate within the vast target population of millions of users could be practically lucrative and it is extremely easy to reach and attack these unsuspicious users. As social networks explode in popularity and adoption rates, the perception of trust is implied throughout interactions and relationships that take place within these platforms. Consequently, malware attacks that exploit the perceived trust placed on friends are a frequent occurrence.

Collectively, the types of malware threats and attacks to today's social media networks include Trojan horses, adware, spyware, viruses and worms, rootkits, keyloggers, ransomware, bots and/or botnets, and puppetnets (Brunty et al., 2014; Timm & Perez, 2010). Trojan horses are designed to appear legitimately useful programs. Nevertheless, in reality, they are malicious as they can infect systems and cause serious damages. For example, they can delete or encrypt files and thus cause data loss. Furthermore, they can copy themselves to shared files and infect other systems (Al-Hamami, 2014). Rootkits are propagated through infected sites or system installations. They may exploit OS or browser vulnerabilities to illegally capture data or impersonate user actions for the compromised device. Keyloggers also exploit OS or browser vulnerabilities, and steal stealthily steal sensitive user data like passwords (Morabito, 2016).

Active social media usage has been exponentially growing over years. Consequently, attackers understand that social networks have many users who can easily become bots for use in botnets. In addition, these networks have huge volume and high velocity content that may be used to conceal illegitimate and malicious traffic. This may become a botnet's CNC.

Research has shown that cases of social networks (like Twitter and Tumblr) used as botnets (Thomas & Nicol, 2010; Timm & Perez, 2010). How do these attacks happen? Basically, the CNC (in this case a social network) is leveraged to issue as sets of commands to bots (users) and infect them with malware. The attacker creates a fake social network account in addition to their bots that carry the attack commands. Once a system gets infected, the attacker uses the CNC to instruct the bots to launch further attacks, including targeted spamming, data and identity theft, data deletion, extortion and ransomware, file or HDD encryption and others. Koobface is an example of a bot that used social networking sites (like Facebook, MySpace, and Twitter) for propagation purposes.

Installing software on user machines so as to infect them could require a lot of time. Additionally, it could leave a trace. Would it not be amazing if an attacker recruits several systems and infect them without actually installing software? Attackers have been able to achieve this awesome technique to gain access to billions of people sharing diverse social networks with limitless trust. Puppetnets are the next-gen botnets that are allowing malware writers recruit systems while they are logged into a site. An attractive, yet malicious page is created to appeal to as many people as possible. The page is then programmed with the content that will be distributed to unsuspecting browsers in a concealed manner to prevent the user from detecting a potentially malicious plan. The page is published and its link placed on social media forums. Every user who visits the malicious page becomes the attacker's puppet. Then, the hidden control commands are executed to automatically launch the pre-configured attacks (Faghani & Saidi, 2009; Thomas & Nicol, 2010; Timm & Perez, 2010).

It is evident that social media networks represent a very promising platform for tricking any number of persons into visiting the malicious page. Which other forum would such criminals use to trick millions of users with much ease and success other than social media? Social media is the best place where absolute freedom of information sharing and distribution is guaranteed and millions of unwary people can be tricked by malware writers. It is these social networks that botnet and puppetnet writers leverage as a highly accessible, concealing, affordable and flocked infrastructure for successfully completing their attacks.

So, what is the difference between botnets and puppetnets? Botnets require a Trojan installation on a victim's system to convert them into a bot. On the contrary, puppetnets do not such an installation. Instead, a malicious Web page is used to recruit users as bots. The users are then removed as bots upon navigation away from the malicious page. Puppetnets are also better placed to conceal their actions as they expire when the browser has been closed (Timm & Perez, 2010). Therefore, more advanced and proactive malware defense controls should be continually developed to address the ever-evolving threats.

The Viral, Pervasive and Dynamic Nature of Social Media Networks

Individuals, groups and organizations from all over the world are increasingly becoming active users of social media platforms. As more and more people engage and interact with these technologies, attackers have unsurprisingly found their malicious tasks simplified (Dunham, 2008). Unknowingly, users place a lot trust in these highly pervasive networks and criminals are aggressively coming up with tools and techniques for use in hiding their malware attacks. At the same time, social media platforms are inherently viral and tracking down attackers is problematic

(Thomas & Nicol, 2010; Timm & Perez, 2010; Yan et al., 2011). Therefore, criminals are using these platforms to quickly spread massive loads of malware.

The dynamic nature of Web 2.0 has made social networking amazing thanks to improved levels of communication, participation, content generation, and information sharing. Social networking over these Web 2.0 technologies equally empowers attackers to actively introduce their loads into online networks that are very accommodating in relation to collection and distribution of information, expression of ideas, collaboration and other functions (Sophia van Zyl, 2009; Timm & Perez, 2010).

Major Vulnerabilities in Social Media Networks and Third-Party Apps

Social media technologies may come with programming flaws and/or errors that could be exploited to launch malware-related attacks. Popular social media platforms have suffered these types of attacks and criminals may continue striking severally in the future. XSS attacks are the most prevalent programming flaws that have been successfully compromised the security of a number of social networking networks, for instance, Twitter and MySpace. Allowing tag inputs allowed attackers to influence users distribute bad links to others who would be equally in danger (Al-Hamami, 2014). “Samy”, Code Red I, Code Red II, and Slammer are perfect examples of worms that exploited XSS weaknesses in MySpace.com and Twitter among other social media platforms (Al-Hamami, 2014; Faghani & Saidi, 2009; Timm & Perez, 2010). Therefore, social media operators should constantly improve their security functionalities and introduce new ones to tackle unresolved weaknesses.

There are several “cool” third-party apps that offer compelling services like instantaneous sharing of photos and receiving notifications. These apps make the online social landscape more enjoyable. What if these apps could be used to launch malware attacks? That would be rather scary, but users do not recognize the fact that they risk falling victims. Criminals may exploit vulnerabilities within the genuine apps to breach information security (Al-Hamami, 2014).

Rogue Third-Party Apps

Many rogue third-party apps flock the social media today. Most of these are built by criminals to compromise users using attacks such as like-jacking, click-jacking, and share-jacking. They trick unsuspicious users into liking, clicking or sharing something without their consent. Basically, social engineering tools and techniques like phishing and spamming as the initial strategies to trick social media subscribers into trusting unsolicited requests and offers (Thomas & Nicol, 2010). Clickjacking malware especially starts with a false notification about the need to download and install a system clean up solution or a mandatory upgrade.

Adware, drive-by downloads, and “malvertisements” may be used to influence decisions and actions to install malware, create fake user or corporate profiles, or send corrupt messages. These malware uses buttons like “Next” or “Cancel” to implement “like”, “share” and such features that promote propagation of worms (Abraham & Chengalur-Smith, 2010). The impact could range from experiencing unwanted annoying adware to distressing viruses, worms, rootkits, keyloggers, botnets and Trojans in that they may lead to data theft, data modification, extortion, and DoS and DDoS among others.

Social Networking Malware Security Risks

Insights derived from past studies shows that an increase in social media presence and usage increases the likelihood of contracting malware infections. Over years, social media malware threats have moved beyond common worms and viruses to disastrous attacks like ransomware and puppetnets (Bahadur et al., 2011). Introduction of malware to users' systems like Web browsers, operating systems, machines, servers, and networks may lead to the following major risks: annoyance, extortion and fraud, threats, data theft and leakage, "owned" or hijacked systems, disruption of systems, damaged reputation, and financial liability. For example, botnets may be used to propagate ransomware intended to encrypt files and demand a particular fee so that the victims can regain access to their invaluable data. Moreover, ransomware victims may face threats that their stolen or leaked information will be published (Thomas & Nicol, 2010).

Protection Against Social Networking Malware Security Risks

Secure Internet technologies constitute an essential protection measure against the current and future social media malware-related threats. These controls range from security devices such as firewalls and software as anti-virus programs that may help check, delete, and log viruses, worms, and Trojan horses among other types of malware that may exploit browser, social media or third-party app vulnerabilities. Other essential technologies include Web and content filters, proxy servers, and Web gateways (Timm & Perez, 2010; Yan et al., 2011; Zurkus, 2016). Firewalls monitor incoming and outgoing connections for block potentially malicious traffic. Proxy servers and/or Web filter tools help detect and block executables, while content filters maybe used to implement social media usage restrictions. It is good practice to use the acceptable social media use policy as the basis for configuring content filters. In addition, all technologies should have proven malware protection effectiveness and they should be kept up-to-date through application of frequently released updates and patches.

Anti-virus and firewall systems are considered inadequate malware security technologies within the social media landscape. The fact that these systems depend on inflexible policy and signature strategies makes them unsuitable for social media applications that are uniquely mobile, viral, pervasive and dynamic in nature (Joe & Ramakrishnan, 2014; Zurkus, 2016). What if a new link without a known signature is placed on social media? Definitely, a zero-day attack would be successful because antivirus and firewall systems may not detect it. Therefore, it is important to deploy securely configured Web gateways to facilitate on-the-fly content analysis as opposed to looking for well-known payloads or signatures.

Organizations continue to flock social media networks to drive greater efficiencies in PR, customer service, sales and marketing, relationships and loyalty initiatives, CSR, partnerships, and employee relationships among other strategic business areas. Nevertheless, they are placing little emphasis on potentially severe malware security vulnerabilities and threats in their IT risk assessment and scoring efforts. This is despite the fact that malware propagated through social media has been on the rise with increased adoption of these networks (Faghani & Saidi, 2009; Picazo-Vela et al., 2012; Zurkus, 2016). Therefore, organizations should prioritize malware risk by assessing the likelihood of malware infections, threat impact severity, and overall risk levels. Such an understanding would inform better decisions regarding effective defense measures against social networking malware. According to Morabito (2016), organizations should also regularly assess malware-related threats that may emanate from social media to make sure they proactively fight emerging threats.

Malware security technologies should be accompanied by an appropriate acceptable social media usage policy. The policy should communicate and enforce acceptable practices in relation to social media usage, including networking and/or connecting with friends and colleagues internally and externally in addition to emailing and texting. On the other hand, downloading apps from social networks is one of the least acceptable social media usages

(Bahadur et al., 2011). The policy should incorporate a set of dos and don’ts in addition to best practices, procedures, and guidelines towards promoting secure social networking practices in the workplace and beyond (Bahadur et al., 2011; Yan et al., 2011). Moreover, proper enforcement should be pursued to motivate stakeholders to comply with defined policy requirements. Other crucial considerations for an effective social media policy include good leadership and governance and assurance of resources such as IT security personnel and defense technologies (ISACA, 2010).

Social media training and awareness is essential as it provides the first “line of defense” against malicious codes that stand to be propagated on Internet-mediated networking platforms. Basically, it plays a major role in bridging existing gaps in malware security skills and awareness (Picazo-Vela et al., 2012; Thuraisingham et al., 2016). For example, attacker attempts to trick users using disguised third-party apps and spam links will have minimal chances of success since target victims are empowered to recognize potential threats and act accordingly. Trust issues that are prevalent on social networks may be resolved if users learn to detect fraudulent messages and use alternative approaches to contact their friends or organizations to ascertain the authenticity of any suspicious message (Al-Hamami, 2014). With effective training, there are higher chances of achieving successful malware protection results for individuals and organizations with a social media presence (Bahadur et al., 2011; Gao et al., 2010). Skilled and security-conscious users are more careful when interacting with potential insecure elements such as unsolicited links, unknown apps, and suspicious alerts because raising awareness promotes positive behavioral changes. In turn, it heightens security.

Future Research Recommendations

Evidently, social media networks are easy to access and use across diverse computing devices, ranging from PCs to smartphones and tablets. Moreover, there are wide array of social media platforms and services at the disposal of users irrespective of geographical location provided one has a supported device and internet connection. Consequently, millions of individuals and organizations continue to flock social networks to realize communication, collaborative, interactive, and engagement and other benefits. This has made these platforms become widely used globally and a lot of traffic is shared on here.

Malware writers have also established social media presence because it has become a “gold mine” for their ends. They breed and propagate various malicious codes within and through these globally accepted networks. As a result, social media growth has been associated with a surge in malware attacks. Moreover, individuals and organizations have seen cybercriminals breach various types of targets, for example, personal and corporate social media accounts and/or profiles, operating systems, Web browsers, and machines (desktops and mobile devices) and computer networks. Therefore, criminals have recognized social media as the next big thing from the perspective of malware attack vectors.

Individuals and organizations should understand that social networks are one of the most sensible targets for malware writers. Oftentimes, hackers and other cybercriminals prioritize social networks as they assure accessibility to a large pool of users who can easily be compromised in part due to unawareness. Users ought to acknowledge that they are targeted by criminals out to exploit social networks and lack of adequate awareness, and pursue appropriate defense measures.

However, what are the fundamental rules for individuals and organizations with social media presence? To start with, individual social media users should consider the following fundamental rules:

- Carefully deal with all links received from friends since some may be sent by criminals disguised as friends.
- Do not accept any software and update requests and/or alerts received from suspicious entities because they may be originating from criminals out to inject some malware once downloaded or installed. Br careful when downloading and installing apps from social networks.
- Do not trust all messages to be coming from who they claim to be from. Instead, the sender of suspiciously fraudulent message should be contacted using a different method to confirm its legitimacy and avoid falling victim to criminal tricks.
- Any URL to the personal social media account should be typed or pasted directly into the Web browser. This avoids the risk of clicking a malicious link that redirects you to a contaminated site.
- Be rational when accepting friends since some may be fake accounts implemented through bots and botnets.
- Comply with work-related acceptable social media use policy.

Organizations should consider the following fundamental rules to stay secure from malware attack related to social media presence and use:

- Ensure that enterprise social media accounts and/or profiles are based on best security practices, including aspects of being professional and run by skilled personnel.
- Prioritize social networking malware security in risk assessment, scoring, and defense considerations.
- Implement proven Internet, host or device, and network technologies (such as antivirus software, firewalls, Web filters and Web gateways) to ensure proactive detection and prevention of malware. Ensure that these technologies are frequently updated to prevent and mitigate zero-day exploits.
- Formulate an acceptable social media policy and communicate it. All stakeholders should also be trained on best practices and procedures promoted by the policy. Other policy considerations include good leadership, adequate resourcing, and enforcement.
- Constantly monitor social media activities one enterprise accounts/profiles to ensure they have not been hijacked by criminals to disseminate unwanted messages.
- Emphasize social media security awareness education and campaigns to communicate potential risks to employee and to promote security-conscious behaviors and practices, which eventually lead to heightened security.

Continued usage of social media by organizations can lead to considerable cultural and procedural changes, especially in communication and engagement areas (Morabito, 2016). Introduced changes should be actively managed, monitored and measured so as to ensure that maximum value is realized and malware risks minimized as much as possible. However, insignificant research has been carried out to provide insights into ways through organizations can maximize the value or benefits of social media usage and reduce associated malware risks using established information security frameworks. This attracts the following research questions that future researchers should consider.

New Research Question 1:

What is the correlation between the strategic benefits of leveraging social media and the malware risks involved?

Evidently social media has many strategic benefits to individual users and organizations. Some of these include improved social connectedness, engagement, marketing, business relationships with various stakeholders, recruitment, CSR, loyalty program effectiveness, customer service and revenue performance. On the contrary, existing research indicate that malware threats have been on the rise with proliferation of social media platforms and adoption rates. Malware attacks may lead to serious risks such as data theft or leakage, ruined reputation and revenue loss. However, it is not clear whether the benefits social media outweighs the malware risks associated with its continued usage.

New Research Question 2:

How can established information security frameworks (like COBIT and ISO 27000 series) be used to inform decisions regarding social media malware risks and defense?

Organizations rely on established IT security frameworks (such as COBIT and ISO 27000 series) to clearly understand controls, processes and procedures that form sound governance in relation to a specific technology under consideration. While such frameworks have been widely used in domains such as user, application/software, LAN/WLAN, and remote access, they are yet to be utilized to inform risk and defense decisions in the context of social media usage. Therefore, this question will help ascertain how COBIT and other IT security frameworks may be used to come up with an effective strategy to safeguard against social media risks. It will deliver insights that may be prioritized to run successful social media strategy in the era of surging malware threats to information security.

New Research Question 3:

What are the legal and regulatory requirements that apply to social media and malware attacks?

Technologies and innovations are commonly accompanied by a number of legal and regulatory requirements that seeks to assure information security and privacy. However, this research has not covered issues related to law and regulations with respect to social media usage. Of course, social networks attract vulnerabilities, but the viral nature of these platforms may inhibit efforts to track down perpetrators of malware attacks. Therefore, it is important to clearly understand the possible options that apply in case an individual or an organization is affected by a malware attacks executed using social media. The question will help promote compliance with existing laws and regulations, which is crucial to any technology governance initiative.

References

Abouzakhar, N. (Ed.). (2015, July). ECCWS2015-Proceedings of the 14th European Conference on Cyber Warfare and Security 2015: ECCWS 2015. Academic Conferences Limited.

Abraham, S., & Chengalur-Smith, I. (2010). An overview of social engineering malware: Trends, tactics, and implications. *Technology in Society*, *32*(3), 183-196.

Al-Hamami, A. H. (Ed.). (2014). *Handbook of Research on Threat Detection and Countermeasures in Network Security*. IGI Global.

Ariel, Y., & Avidar, R. (2015). Information, interactivity, and social media. *Atlantic Journal of Communication*, *23*(1), 19-30.

Ashley, P., Lee, C., & Stabler, C. (2014). Addressing Emerging Threats and Targeted Attacks with IBM Security Network Protection. IBM Redbooks.

Athanasopoulos, E., Makridakis, A., Antonatos, S., Antoniades, D., Ioannidis, S., Anagnostakis, K., & Markatos, E. (2008). Antisocial networks: Turning a social network into a botnet. *Information security*, 146-160.

Bahadur, G., Inasi, J., & De Carvalho, A. (2011). *Securing the Clicks Network Security in the Age of Social Media*. McGraw-Hill Osborne Media.

Baltazar, J., Costoya, J., & Flores, R. (2009). The real face of koobface: The largest web 2.0 botnet explained. *Trend Micro Research*, *5*(9), 10.

Batten, L., Li, G., Niu, W., & Warren, M. (2014). *Applications and Techniques in Information Security*. Springer Verlag.

Brunty, J., Miller, L., & Helenek, K. (2014). *Social media investigation for law enforcement*. Routledge.

Caviglione, L., Coccoli, M., & Merlo, A. (Eds.). (2013). *Social Network Engineering for Secure Web Data and Services*. IGI Global.

Ciampa, M. (2012). *Security+ guide to network security fundamentals*. Cengage Learning.

Dunham, K. (2008). *Mobile malware attacks and defense*. Syngress.

Dooley, M., & Rooney, T. (2017), DNS Security Management. John Wiley & Sons.

Faghani, M. R., & Saidi, H. (2009, October). Malware propagation in online social networks. In *Malicious and Unwanted Software (MALWARE), 2009 4th International Conference on* (pp. 8-14). IEEE.

Filiol, E., & Erra, R. (2012). *Proceedings of the 11th European Conference on Information warfare and security: ECIW 2012*. Academic Conferences Limited.

Furnell, S., & Clarke, N. (2007). *Proceedings of the International Symposium on Human Aspects of Information Security & Assurance (HAISA 2007)*. Lulu. com.

Gao, H., Hu, J., Huang, T., Wang, J., & Chen, Y. (2011). Security issues in online social networks. *IEEE Internet Computing*, *15*(4), 56-63.

Gao, H., Hu, J., Wilson, C., Li, Z., Chen, Y., & Zhao, B. Y. (2010, November). Detecting and characterizing social spam campaigns. In *Proceedings of the 10th ACM SIGCOMM conference on Internet measurement* (pp. 35-47). ACM.

Green, M. J. S. (2015). *Cyber Security: An Introduction for Non-Technical Managers*. Ashgate Publishing, Ltd.

Hajirnis, A. (2015). Social media networking: Parent guidance required. *The Brown University Child and Adolescent Behavior Letter*, *31*(12), 1-7.

Hämmerli, B. (2007). *Detection of Intrusions and Malware, and Vulnerability Assessment: 4th International Conference, DIMVA 2007 Lucerne, Switzerland, July 12-13, 2007 Proceedings*. Springer Science & Business Media.

Harkins, M. (2012). *Managing risk and information security: protect to enable*. Apress.

He, W. (2013). A survey of security risks of mobile social media through blog mining and an extensive literature search. *Information Management & Computer Security*, *21*(5), 381-400.

Hekkala, R., Väyrynen, K., & Wiander, T. (2012, June). Information Security Challenges of Social Media for Companies. In *ECIS* (p. 56).

ISACA. (2010). Social Media: Business Benefits and Security, Governance and Assurance Perspectives [Whitepaper]. Retrieved from http://www.isaca.org/groups/professional-english/security-trend/groupdocuments/social-media-wh-paper-26-may10-research.pdf

Johnson, M. (2016). *Cyber Crime, Security and Digital Intelligence*. Routledge.

Joe, M. M., & Ramakrishnan, D. B. (2014). A survey of various security issues in online social networks. *International Journal of Computer Networks and Applications*, *1*(1), 11-14.

Kaplan, A. M., & Haenlein, M. (2010). Users of the world, unite! The challenges and opportunities of Social Media. *Business horizons*, *53*(1), 59-68.

Kayem, A. (Ed.). (2014). *Information Security in Diverse Computing Environments*. IGI Global.

Labuschagne, W. A., & Veerasamy, N. (2013, July). Dangers of Social Networking Sites□the Propagation of Malware. In *Proceedings of the 12th European Conference on Information Warfare and Security: ECIW 2013* (p. 173). Academic Conferences Limited.

Leavitt, N. (2011). Mobile security: finally a serious problem. *Computer*, *44*(6), 11-14.

Liaropoulos, A., & Tsihrintzis, G. (2014). *ECCWS2014-Proceedings of the 13th European Conference on Cyber warfare and Security: ECCWS 2014*. Academic Conferences Limited.

Management Association, Information Resources (Ed.). (2015). *Social Media and Networking: Concepts, Methodologies, Tools, and Applications: Concepts, Methodologies, Tools, and Applications*. IGI Global.

Morabito, V. (2016). *The future of digital business innovation: Trends and practices*. Springer.

Obar, J. A., & Wildman, S. S. (2015). Social media definition and the governance challenge: An introduction to the special issue. *Telecommunications policy*. *39*(9), 745–750.

Picazo-Vela, S., Gutiérrez-Martínez, I., & Luna-Reyes, L. F. (2012). Understanding risks, benefits, and strategic alternatives of social media applications in the public sector. *Government information quarterly*, *29*(4), 504-511.

Sanzgiri, A., Hughes, A., & Upadhyaya, S. (2013, September). Analysis of malware propagation in Twitter. In *Reliable Distributed Systems (SRDS), 2013 IEEE 32nd International Symposium on* (pp. 195-204). IEEE.

Sophia van Zyl, A. (2009). The impact of Social Networking 2.0 on organizations. *The Electronic Library*, *27*(6), 906-918.

Spencer, T. (2013). *Personal Security: A Guide for International Travelers*. CRC Press.

Statistica. (2017). Global Social Media Ranking 2017. Retrieved from https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users

Thuraisingham, B., Abrol, S., Heatherly, R., Kantarcioglu, M., Khadilkar, V., & Khan, L. (2016). *Analyzing and Securing Social Networks*. CRC Press.

Thomas, K., & Nicol, D. M. (2010, October). The Koobface botnet and the rise of social malware. In *Malicious and Unwanted Software (MALWARE), 2010 5th International Conference on* (pp. 63-70). IEEE.

Timm, C., & Perez, R. (2010). *Seven deadliest social network attacks*. Syngress.

Tipton, H. F., & Nozaki, M. K. (2012). *Information Security Management Handbook* (6th ed.). CRC Press.

Turban, E., Whiteside, J., King, D., & Outland, J. (2017). *Introduction to Electronic Commerce and Social Commerce*. Springer.

UcedaVelez, T., & Morana, M. M. (2015). *Risk Centric Threat Modeling: Process for Attack Simulation and Threat Analysis*. John Wiley & Sons.

Waters, J. K. (2011). Keeping It Clean: Introducing Online Social Media into Your Educational Mission Brings You Right into a Hacker's Bull's-Eye, Can You Ensure Your Learning Environment Stays Uninfected?. *THE Journal (Technological Horizons In Education)*, *38*(1), 52.

Yan, G., Chen, G., Eidenbenz, S., & Li, N. (2011, March). Malware propagation in online social networks: nature, dynamics, and defense implications. In *Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security* (pp. 196-206). ACM.

Zurkus, K. (2016, August 29). Social media, the gateway for malware. CSO. Retrieved from http://www.csoonline.com/article/3106292/social-networking/social-media-the-gateway-for-malware.html