Proceedings of the Informing Science + Information Technology Education Conference

An Official Publication of the Informing Science Institute
InformingScience.org

InformingScience.org/Publications

July 31 - August 5 2017, Ho Chi Minh City (Saigon), Vietnam

ENTERTAINING WHILST DEFACING WEBSITES: PSYCHOLOGICAL GAMES FOR HACKERS

Ashish K Das*	RMIT University, HCMC, Vietnam	ashish.das@rmit.edu.vn
Quynh T Nguyen	RMIT University, HCMC, Vietnam	quynh.nguyenthi@rmit.edu.vn
Susan Thomas	RMIT University, HCMC, Vietnam	susan.thomas@rmit.edu.vn

*Corresponding author

ABSTRACT

Aim/Purpose	This study aims to investigate various characteristics from both victims as defaced websites and defacers that linked to a risk of being defaced through a set of descriptive analysis.
Background	The current figures from a spectrum of sources, both academic and non-academic reports, proved a progressive increase of website defacement attacks to numerous organisations.
Methodology	This study obtains a set of data from Zone-H site, which is accessible to the public, including 99,437 defaced websites. The descriptive analysis is applied in order to understand the motives of defacers and the probability of website re-defacements through the statistical investigation.
Findings	The motives for defacing websites are driven mainly due to entertaining reasons. This in turn has an implication on the type of techniques defacers attack websites.
Keywords	defacement, re-defacement, entertainment and defacer

BACKGROUND

With an increase in the use of the Internet as well as the number of computers connecting to it, the opportunities for cybercrime, such as hacking, virus/worm attacks, Internet time theft data diddling, email bombing, and web defacement, has massively increased and this is evidenced through the numerous attacks that are purported on a daily basis. Remarkably, the CEO of McAfee even stated that cybercrime has internationally beaten the value of the illegal drug trade (Bose & Leung, 2014). Amid all the categories of cybercrime, website defacement is considered as the fastest growing menace to various organisations, from non-profit to financial corporations (Rupley, 2005). A survey conducted

Accepting Editor: Eli Cohen | Received: November 30, 2016 | Revised: March 14, April 14, 2017 | Accepted: April 15, 2017
Cite as: Das, A. K., Nguyen, Q. T., & Thomas, S. (2017). Entertaining whilst defacing websites: Psychological games for hackers. *Proceedings of the Informing Science and Information Technology Education Conference*, *Vietnam,* pp. 1-9. Santa Rosa, CA: Informing Science Institute. Retrieved from http://www.informingscience.org/Publications/3721

by the Computer Security Institute and Federal Bureau of Investigation reported that 90% of the organisations that partook in a study experienced website defacements in 2001 (BBC News, 2002). According to the study by Jones, Kovacich, & Luzwick (2002), website defacement is popular and becomes a disruptive attack to a point that many sites archive up-to-date minute reports on lists of defaced websites on a daily basis.

Web defacement occurs when a perpetrator accesses a website and modifies its contents by inserting malicious links and pop-up windows (Cross et al., 2007). Through the act of vandalism, defacers desire to scrutinise the security weakness or vulnerability of various websites (Viswanathan & Mishra, 2016). The fundamental idea behind such action is that the perpetrators endeavour to embarrass website owners and eventually exert direct negative impacts on the attacked organisations, or individuals, and consequently affecting their related stakeholders, such as clients and distributors. This leads to financial damages and damage to an organisation's reputation. The latter is an intangible asset, the losses of which are difficult to quantify in monetary terms (Kosina, 2012). Due to the nature of the defacement act, some experts labelled website defacement as a virtual graffiti activity: the most scandalous example of this being the defacement series that occurred when Hitler images were displayed on the Georgia Parliament website (Hopkins, 2016; Takahashi, 2008).

Recently, web hosting companies and cyber security bodies have released toolkits and online monitoring systems in order to detect defacement incidents with the aim of tightening the security performance levels to minimise the risks of attack by smart defacers. However, the number of defaced websites, as well as other cyber incidents, are still on the rise and, globally, there is a lack of in-depth research and analysis on its technical aspects (Kuypers, Maillart, & Paté-cornell, 2016). Hence, it is important to develop a descriptive statistical analysis, including defacing techniques, types of affected systems and victims. This would act as a novel contribution to tackle the defacement problem and further improve security interventions focusing on cybercrime and malicious attacks. Furthermore, this study will contribute to the knowledge of policy makers of the scale and nature of cybercrime and move forward towards establishing a legitimate framework, with a sound evidence base, for tackling defacement attacks.

The aim of this study is to analyse the defacement incidents and its related factors and motives through descriptive statistics.

ARCHIVES DESCRIPTION METHODOLOGY

Website defacement has been around since the Web technology was established, with sources reporting that such activity commenced as early as 1995 (Oriyano, 2014). There are many public archives that record and store sites that have been defaced (Bidgoli, 2005). One such example is Attrition.org. Another archive, Zone-H is considered to be one of the leading repositories that has recorded defaced incidents since 1998 (Zone-H, 2014). Following the receipt of a notification from an attacker, Zone-H conducts an investigation to ensure that indeed there was a defacement incident and, as a result, it regularly lists and officially publishes details of the defaced websites. Thus, Zone-H collects defacement data directly from the defacers and releases thousands of announcements each day. In order to check the validity of claims, Zone-H deploys its own detection algorithms and, in return, robots take screenshots of the defaced websites as evidence and stores them as mirrors.

As the leading archiving site, Zone-H classifies the virtual graffiti activities into two types of defacement, based on the characteristics of domains, including normal and special typologies, with special defacements consisting of special domains, such as governmental and security agencies. With regard to the technicality aspect, there are four types of defacements, namely homepage, mass, re-defacement and special defacements (Zone-H, 2014). Ultimately, the extracted data set comprises 16 parameters, such as date of the defacement incident, attacker's name and ID, domain of the targeted website, as well as its IP address(es), geographical location, web server typologies where the target website is hosted, motivations for the attack, techniques used for website defacement, type of defacement and re-defacement occurrences.

The descriptive analysis of this study acts as an impetus for a larger study in order to understand the motives of defacers and the probability of website re-defacements through the statistical investigation.

DATA DESCRIPTION

This study acquired data recorded during the period 1-31 December 2012 from Zone-H. The dataset included a sample of N= 99,437 incidents, including both successful normal and special website defacements in 145 countries. On a daily basis, the pattern of defacements fluctuated between 1,572 and 5,246 occurrences. Even though the number of defacements from the data set on a daily basis is diverse, accounting by the rate of defacement frequency, it displayed an increasing trend towards the end of the month.

The average of number of attacks on daily basis was approximately 3,200 incidents. Based on this as the daily average rate for the entire year of 2012, the trend for website defacement would have risen 120 times in 11 years since Nugent and Raisinghani's (2002) study in 2001, which used data from the Attrition archive and reported an average daily rate of 30 defacement occurrences. This escalating trend strengthens the fact that defacement has become a popular and real Internet security threat to organisations and individuals alike, with particularly special consequences in the E-commerce field.

During the above-stated one-month period in December 2012, the US, alone, was subjected to 36,571 website defacement attacks, which is approximately 11 times higher than the average rate. The gap differentiating the US from other countries is substantially large since the US claimed 36.8% of the defacement attacks in that month, while the second-placed Germany claimed only 6.5%. From this initial observation, it could be concluded that North America experienced the highest number of website defacements, followed by Europe. These were followed in decreasing order by Asia (led by Thailand), South America (led by Brazil), Africa (led by South Africa) and Oceania with Australia as the country with the highest occurrences of defacement. These countries share some similar characteristics, examples of which being relatively strong economies and large Internet usage. Noticeably, China and Russia did not appear in the top 5 countries for website defacement attacks.

FINDINGS FROM THE DESCRIPTIVE ANALYSIS

Based on the studied dataset and the frequency of attacker ID variable, there were 2,241 hackers during that month of December 2012. The defacer with ID Hmei7 was the strongest attacker compared to all others, since the related attacks amounted to 13,405 websites – i.e., 4 times higher than the daily average for that month – across 124 countries. Furthermore, Hmei7 was likely to be the most active defacer since the defacing activity was carried out on a daily basis. The highest number of website defacements occurred on the 29th with 1,734 incidents. Approximately, 61% of all the defaced websites by Hmei7 were mass defacements. Hmei7 seemed to deploy predominantly the file inclusion technique in order to vandalise the target websites with a percentage of 98.55% in comparison with other used techniques, such as web server external module intrusion (0.36%), mail server intrusion (0.33%), social engineering (0.11%) or configuration/admin.mistake (0.1%). Besides, the central motives for Hmei7 to deface various websites appeared to be mainly for entertainment purposes (99.27%) with a minute element for revenge against some websites (0.59%).

The study revealed that there were 22 types of web servers involved in the defacement attacks (Table 1), with the Apache server considered as the most popular target, at approximately 73% of all attacks. In terms of operating systems, Linux appeared to be the most victimised amongst the 15 operating systems used during that month. These findings are perhaps due to the fact that the Apache web server is installed on a Linux platform and is one of the most commonly used servers on the Internet (Wang & Robey, 2016). Some others sources stated that Apache and Microsoft IIS by far hold 90% of the web servers market share (Cross et al., 2007; Netcraft, 2012). Incidentally, this fact coincides with the finding from the study where the cumulative proportion of Apache and IIS Servers involved in defacement incidents was also in excess of 90% of the total occurrences.

Table 1. Web Server Types and Operating Systems Involved in the Defacement Incidents

Name Server	Frequency	Percent	Frequency	Percent	Name OS
Apache	**72650**	**73.128%**	**76208**	**76.709%**	***Linux***
IIS/6.0	13628	13.718%	13897	13.988%	*Win 2003*
IIS/7.5	1632	1.643%	2968	2.988%	*Win 2008*
IIS/7.0	1057	1.064%	190	0.191%	*Win 2000*
IIS/5.0	192	0.193%	17	0.017%	*Win 2012*
IIS/5.1	7	0.007%	9	0.009%	*Win XP*
IIS/8.0	34	0.034%	2552	2.569%	*Unknown*
Nginx	7525	7.574%	1938	1.951%	*FreeBSD*
LiteSpeed	1399	1.408%	895	0.901%	*F5 Big-IP*
Lighttpd	104	0.105%	660	0.664%	*Solaris 9/10*
NOYB	65	0.065%	8	0.008%	*MacOSX*
ATS	45	0.045%	2	0.002%	*Cisco*
Zeus	44	0.044%	1	0.001%	*Citrix Netscaler*
IdeaWebServer	37	0.037%	1	0.001%	*HP-UX*
Others	928	0.932%	1	0.001%	*IRIX*
					Total
Total	99347	100.000%	99347	100.000%	

Others: Unknown (N=879, 0.903%), GSE (N=4, 0.004%), IceWarp (N=2, 0.002%), Microsoft–HTTPAPI (N=2, 0.002%), Rapidsite (N=2, 0.002%), Ultraseek (N=2, 0.002%), ConcentricHost-Ashurbanipal (N=1, 0.001%), YTS (N=18, 0.018%).

As stated above, although Zone-H classified defacement into four types, Balakrishman (2007), on the other hand focused on three classifications, namely, mass, regular, and re-defacement. In re-defacement, a website is attacked and defaced more than one time. Similar to defacement acts, re-defacement occurs when a perpetrator could either use mass or regular defacement techniques to re-deface a target website. In this study, it emerged that the defacement incidents that occurred in that month were skewed toward mass attacks with a proportion of 75.1% (N=74,571) in comparison to regular defacement. Noticeably, based on the dataset retrieved from Zone-H, it can be shown that, in a single mass-defacement, a perpetrator could successfully deface a cluster of web servers, reaching as many as 1,618 websites (on a home page). The operating system of use in these defaced websites was the Linux operating system in combination with the Apache Server, as an open source software, which enabled a perpetrator to have multiple chances to identify the vulnerability of the system and exploit it far more than in the case of other closed sources.

Amid the 99,347 website defacement incidents, the proportion of re-defacement was 11.9% in the month of December 2012. In other words, the probability of a domain experiencing re-defacement was approximately 12%. In relation to the operating system, as well as the types of web servers that were hosting these target websites, the trends for defacement and re-defacement were similar. These exhibited a gradual decrease, starting from the open-source Linux server to the much less popular

servers, such as Citrix Netscaler, HP-UX and IRIS (Figures 1 & 2). Noticeably, the proportion of re-defacements using the mass technique was much larger than the regular technique, at 71.9%.

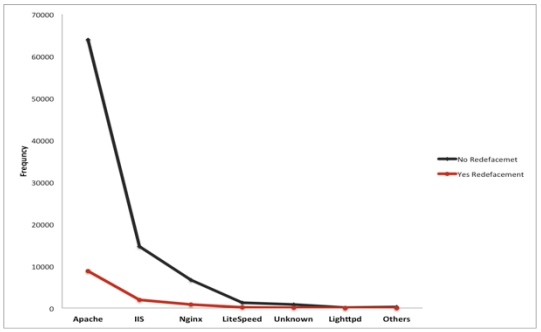

Figure 1: Frequency Between Re-defacement by Web Server Types

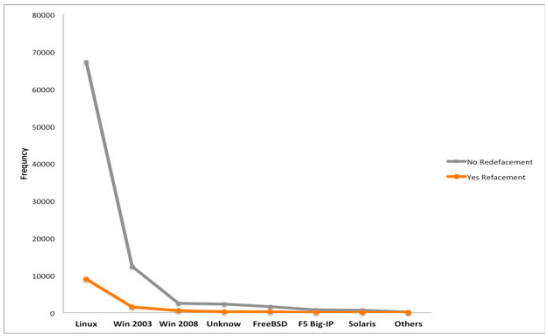

Figure 2: Frequency Between Re-defacement by Operating System Server Hosting Websites

Note: For web server types, other group is comprised of NOYB, ATS, Zeus, IdeaWebServer, YTS, GSE, ICe-Warp, Microsoft-HTTPAPI, Rapidsite, Ultraseek and ConcentricHost-Ashurbanipal. Also, from IIS/5.1 to 8.0 – these versions were grouped as one category, namely, IIS. For operating system grouping, other group includes Win 2000, Win 2012, Win XP, MAC OSX, Cisco, Citrix-Netscaler, HP-UX and IRIX.

In terms of techniques for defacing a web page, the study uncovered that an array of 31 hack-modes were applied in order to vandalise the 99,347 websites, ranging from *file inclusion* (23.9%), *known vulnerability* (13%), *other server intrusion* (10.4%), *SQL injection* (9.9%) to *remote administrative panel access through social engineering* (0.03%). These defacement techniques were classified according to the Zone-H database. The above proportions support the claim of some experts that the *file inclusion*, also sometimes referred to as *remote file inclusion*, technique requires just little hacking skill, knowledge, and time from an intruder; hence this could partially explain the rationale behind its wide usage in website defacement (Nagpal, Chauhan, & Singh, 2005). Other sources proposed that *SQL injection* was also a commonly used method for defacing a web page. The results of this study, however, contended that there were only 9,879 defacement occurrences using *SQL injection*. On the other hand, the proportion of unknown techniques was substantially high, at 12.7%. That latter figure is even higher than the number of incidents identified through the more known techniques, such as *server intrusion* and *SQL injection*. This indicates that perpetrators were likely to apply certain types of unspecified techniques in carrying out defacement.

According to the study conducted by Wendt (2016), defacers possess various motives for justifying their acts of vandalism, such as political reasons, patriotism, religion and revenge. Through various socio-political conflicts at the international level, such as between Koreans and Japanese, Chinese and Americans, and Israelis and Palestinians, the defacers turn cyberspace into a war zone by defacing each other's websites and split into separate groups based on a certain ideology. In the case of this study, Zone-H also archived the motivations of each defacement event, such as for entertainment, political, vengeance, or patriotism reasons, in order to highlight the level of a defacer's skill and ability in hacking societies. The analysis showed that the majority (50.6%) of the reasons for defacement was for entertainment purposes. Coincidentally, the percentage of unknown purpose (12.7%) for website defacement was similar to the percentage of unknown techniques. Combining the occurrences of the techniques that were deployed by perpetrators during that month of 2012, namely, *file inclusion*, *known vulnerability*, and *SQL Injection*, the cumulative percentage for these 3 techniques (46.8%) attained a somewhat similar rate as the entertainment purpose (Table 2). This could lead to

the hypothesis that there might be an association between defacement techniques and perpetrators' purposes.

Table 2. The Valid Percentage of Defacing Reasons and Techniques

Techniques	Percentage (%)	Cumulative Percentage (%)	Cumulative Percentage (%)	Percentage (%)	Purpose of Defacement
File Inclusion	23.9	23.9	50.6	50.6	Entertainment (heh...just for fun!)
Know Vulnerability	13	36.9	65.75	15.1	I just want to be the best defacer
SQL Injection	9.9	46.8	72.2	6.5	Political reasons
Not available	12.7	59.5	84.4	12.6	Not available
Other Server Intrusion	10.4	69.9	91.3	6.5	Revenge against that website
Other Web Application Bug	6.1	76	96.6	5.4	As a challenge
Undisclosed (new)	4.3	80.3	100	3.3	Patriotism
Vulnerability Web Server Intrusion	2.9	83.2			
Configuration / admin.mistake	2.6	85.8			
URL Poisoning	1.9	87.7			
Brute Force Attack	1.7	89.4			
Web Server External Module Intrusion	1.6	91			
SSH Server Intrusion	1.3	92.3			
Others	7.7	100			

The authors of this study attempted to unravel the life span of the targeted websites since the moment of first defacement. An application was developed using Visual studio using C# in order to verify the status of the HttpWebResponse. The testing period took place during the period of 13-24 October 2016. The results revealed that, approximately 4 years following the defacement point, the proportion of websites which were still not in operation was 57%. This implies that the life span of such defaced websites is less than 4 years, counting from the moment of the attacks. The remainder of the websites (43% out of 99,347 websites) were in operation at the time of the testing. By operational, it is meant that the website was displayed either with details/data or strictly as a blank page with a valid domain name. Markedly, the number of defaced homepages that were operational again was more than secondary pages (Figure 3). This perhaps points to the fact that the role of a homepage is seemingly more important than secondary pages; hence organisational or personal effort and financial resources appear to be more attributed to fixing the problems associated with their homepage rather than on secondary pages.

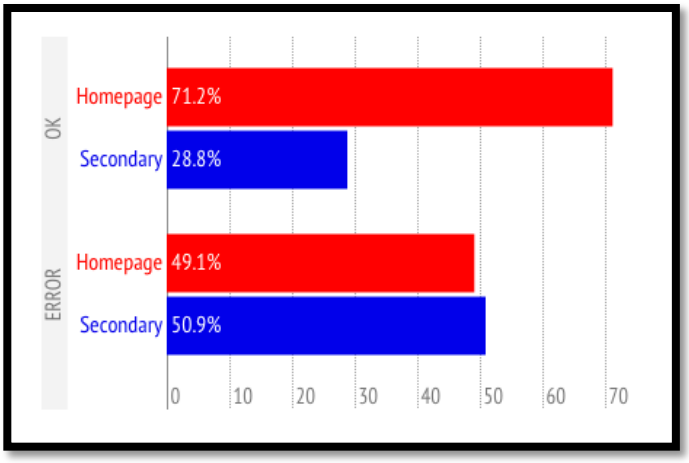

Figure 3. Status of Websites in Relation to Homepage and Secondary Defacement

CONCLUSIONS

Through this descriptive analysis, it emerged that defacers tended to use simple techniques to hack various websites for their entertainment. In addition, defacement incidents occurred in as many as 145 different countries within a month. This reflects the fact that the defacement phenomenon is widespread on a large scale and its repercussions in terms of financial losses have not yet been measured. This may be attributed to a lack of awareness from businesses and firms, including public and private ones, of the necessary financial and human resource investments required for network security. On the other hand, according to Rader and Wash (2015), individuals, regardless of their expertise, do not often acquire formal or informal training related to cyber security and, therefore, at the personal level, the cyber security aspect is not taken seriously into account during Internet usage.

Finally, it must be stated that the study faced a limitation in relation to the dataset. The present analysis was confined to the number of attacks for only one month of a year. Hence, it is a challenge to achieve an objective conclusion for patterns of website defacement and re-defacement. Although faced with such a limitation, the study nonetheless unravelled some initial and useful findings, which can act as a precursor for further research, as well as provide insights for all website owners and website hosting service providers.

RECOMMENDATIONS TO DIGITAL BUSINESS OPERATORS

The findings proved that the intervention is yet to cover all type of website defacement. Once again it reconfirmed the findings of another study by Lagazio, Sherif, and Cushman (2014). They stated in their study that cybercrime has shifted from traditional crimes with the prevalences of viruses in the 1990s to true cybercrimes and cyber platform crimes, including botnets and website defacements. The established existence of vulnerabilities in the World Wide Web has created opportunities for its exploitation, which require little defacement skill. In addition, private firms are prone to have insufficient investment in network security (Gordon, Loeb, Lucyshyn, & Zhou, 2015) and this has become a clear vulnerability that encourages hackers or defacers to easily attack websites.

Also, the defacers are likely to use a set of simple techniques to deface or re-deface the target domains rather than advanced techniques for hacking websites. Hence, organisations, such as website providers and hosting services, need to strengthen the security of their services and systems to not only better improve their levels of security, but also to act in a timely manner to constantly adapt to the ever-evolving technologies and applications.

REFERENCES

Balakrishman, N. (2007). Information technology and communications security in India. In R. Narasimha, A. Kumar, S. P. Cohen, & R. Guenther (Eds.), *Science and technology to counter terrorism* (pp. 31–36). Bangalore: The National Academic Press.

BBC News. (2002). *Computer crime "soaring."* Retrieved November 20, 2016, from http://news.bbc.co.uk/2/hi/science/nature/1916655.stm

Bidgoli, H. (2005). *Handbook of information security, Volume 2, Information warfare, social, legal, and international issues and security foundations*. New Jersey: John Wiley and Sons, Inc.

Bose, I., & Leung, A. C. M. (2014). Do phishing alerts impact global corporations? A firm value analysis. *Decision Support Systems*, *64*, 67–78. Retrieved from http://doi.org/10.1016/j.dss.2014.04.006

Cross, M., Kapinos, S., Meer, H., Muttick, I., Palmer, S., Petkov, P. D., … Temmingh, R. (2007). Web Server and web application testing with BackTrack. In *Web application vulnerabilities: Detect, exploit, prevent* (pp. 283–290). Burlington: Syngress Publishing, Inc.

Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Zhou, L. (2015). Increasing cybersecurity investments in private sector firms. *Journal of Cybersecurity*, *1*(1), 3-17. http://doi.org/10.1093/cybsec/tyv011

Hopkins T. (2016). *The virtual graffiti project*. Retrieved November 20, 2016, from http://www.zone-h.org/news/id/4745?zh=1

Jones, A., Kovacich, G. L., & Luzwick, P. G. (2002). Everything you wanted to know about information warfare but were afraid to ask. In A. Jones, G. L. Kovacich, & P. G. Luzwick, *Global information warfare: How businesses, governments, and others achieve objectives and attain competitive advantages* (pp. 3–29). Florida: CRC Press LLC.

Kosina, K. (2012). *Wargames in the fifth domain*. Universitat Wien. Retrieved from http://kyrah.net/da/wargames.pdf

Kuypers, M. A., Maillart, T., & Paté-cornell, E. (2016). An empirical analysis of cyber security incidents at a large organization. Retrieved from https://fsi.stanford.edu/sites/default/files/kuypersweis_v7.pdf

Lagazio, M., Sherif, N., & Cushman, M. (2014). A multi-level approach to understanding the impact of cyber crime on the financial sector. *Computers & Security*, *45*, 58–74. http://doi.org/10.1016/j.cose.2014.05.006

Nagpal, B., Chauhan, N., & Singh, N. (2005). Defending against remote file inclusion attacks on web applications. *I-Manager's Journal on Information Technology*, *4*(3), 25–33.

Netcraft. (2012). *September 2012 web server survey*. Retrieved February 25, 2017, from https://news.netcraft.com/archives/2012/09/10/september-2012-web-server-survey.html

Nugent, J. H., & Raisinghani, M.S. (2002). The information technology and telecommunications security imperative: Important issues and drivers. *Journal of Electronic Commerce Research*, *3*(1), 1–14.

Oriyano, S. P. (2014). *Hacker techniques, tools, and incident handling* (2nd ed.). Massachusetts: Jones & Bartlett Learning.

Rader, E., & Wash, R., (2015). Identifying patterns in informal sources of security information. *Journal of Cybersecurity*, *1*(1), 121-144. http://doi.org/10.1093/cybsec/tyv008

Rupley, S. (2005). *Beyond viruses*. Retrieved November 20, 2016, from http://www.pcmag.com/article2/0,2817,1848333,00.asp

Takahashi, D. (2008). After the five-day Russia-Georgia war, a chronicle of the cyber battle unfolds. Retrieved November 20, 2016, from http://venturebeat.com/2008/08/12/after-a-five-day-war-a-chronicle-of-the-cyber-battle-unfolds/

Viswanathan, N., & Mishra, A. (2016). Dynamic monitoring of website content and alerting defacement using trusted platform module. In N. R. Shetty, P. N. Hamsavath, & N. Nalini (Eds.) *Emerging research in computing, information, communication and applications* (pp. 117–126). Singapore: Springer Singapore. http://doi.org/10.1007/978-981-10-0287-8_11

Wang, J., & Robey, D. (2016). Social capital in OSS communities: A cross-level research model. In H. Benbya & N. Belbaly (Eds.), *Successful OSS project design and implementation: Requirements, tools social designs and reward Structures* (pp. 87–109). New York: Routledge.

Wendt, D. W. (2016). *Cyber-warfare and the laws of armed conflict: Implications of considering a cyber-attack an act of war.* A Capstone Project Submitted to the Faculty of Utica College April 2016 in Partial Fulfillment of the Requirements for the Degree of Master of Science in Cybersecurity. Utica College.

Zone-H. (2014). *Zone-H unrestricted information.* Retrieved November 20, 2016, from http://www.zone-h.org/archive/special=1

BIOGRAPHIES

Ashish K Das is a Lecturer in Business Information Systems at Royal Melbourne Institute of Technology (RMIT) University Vietnam. He possesses more than 12 years of work experience in software development industry in USA, holding Software and Solutions Architect and Program Manager Positions in various fortune 500 companies and start-ups.

Quynh T. Nguyen (PhD) is a certified IBM SPSS & Modeler specialist and data analytics, having obtained her Master's degree (with Distinction) and PhD from Coventry University, UK, in 2007 and 2016, respectively. She published 31 peer reviewed journals and conferences papers and is an invited speaker at De La Salle University, Manila, Philippines.

Associate Professor **Susan Thomas** received her PhD in Management from University Malaysia and holds dual teaching qualifications from UK and Malaysia. She has more than 20 years teaching experience and has designed more than 200 workshops for Academic Professional Development. She received several awards in teaching and learning, amongst which are Pro Vice Chancellor Award for Teaching, Pro Vice Chancellor Award for Administration, International Graduate Scholar Award, and Best Paper Presented in a Conference. She has published in top tiered journal in the field of education, health care and management. She continues to pursue her passion in community service education, student engagement, scholarship of teaching and learning and leadership in higher education.