MALWARE'S IMPACT ON E-BUSINESS & M-COMMERCE : THEY MEAN BUSINESS !

Pan Juin Yang Jonathan and Chun Che Fung

School of Information Technology, Murdoch University, Perth, Western Australia WA
Jonathan.Pan.JY@gmail.com, l.fung@murdoch.edu.au

ABSTRACT

Malware is a dominant issue in the e-Business arena. It is affecting many of the key e-Business actors from the end users, to businesses offering online services to intermediaries and critical essential infrastructure needed to ensure continued e-Business activities. It has affected the mobility computing platform and m-Commerce too. The impact of Malware is significant and wide ranging. The risk posed by Malware to e-Business actors has prompted variety of responses from the latter. However, the responses have mainly been a catch-up game by the targeted actors (or victims). Beyond the direct impact that Malware has on its targets, there are other forms of reactions that has been induced. Many of which has not been constructive or sufficient. More needs to be done quickly to mitigate the effects of Malware and to encourage the continual and healthy growth of e-Business.

Index Terms — Malware, e-Business, Critical Essential Infrastructure

1. INTRODUCTION

Malware is very much a part of the digital online landscape no matter it is welcome or not. Malware has even been found in outer space with the astronauts [1]. In particular, Malware has been part of the online business world popularly known as e-Business or e-Commerce. e-Business is electronic business activities involving many ICT enabled actors with different roles including business entities (B) and consumers (C). Different permutations of relationship pairs exist in e-Business such as Business-to-Business (B2B), Business-to-Consumer (B2C), and Consumer-to-Consumer (C2C). Among these actors, there are many computing software in the forms of business applications, electronic communication & collaboration, and web tools to facilitate electronic business activities. This paper explores how Malware that exists online has affected e-Business, specifically its actors, directly and indirectly. The paper also provided a discussion on future research direction followed by the conclusion.

2. MALWARE AND E-BUSINESS

e-Business has important contribution to the world economy. e-Business is dependent on the Internet and the Web for its existence and growth. e-Business has also begun to embrace Web 2.0 technologies in a new generation of applications and business models. Beyond the positive contribution that comes from the Internet and the Web, negative contribution in the form of Malware or malicious software has encroached into e-Business. Malware is a major threat to Internet economy according to an Organisation for Economic Co-operation and Development (OECD) report [2]. Malware has caused significant damage to e-Businesses. According to the 2007 report, it noted one survey that estimated US$ 67.2 billion in direct and indirect impact on US businesses alone. Also in the same report and on individual level, it is estimated that US consumers paid up to US$ 7.8 billion over two years to repair or replace their infected systems. Not only is there financial impact from Malware attacks, loss of data or information is significant as this has incurred much indirect damages and inconveniences to the stakeholders in e-business.

In order to better comprehend the extent of impact that Malware has on e-Business, the actors involved e-Business are considered as listed below.

a. End users playing the role of consumers or customers.
b. Commercial organizations or businesses offering services (including sale of products) online.
c. Intermediaries that aid in realizing the e-Business services or transactions such as ISP and payment gateways.
d. Critical Essential Infrastructure operators providing essential supplies like power supply and the communication network.

There are many possible reasons why Malware attacks occur against e-Businesses. They include extortion, corporate warfare or nationalistic reasons. There are different forms of Malware in various forms attacking e-Business. According to Khusial and McKegney [6], the various forms are:

a. Tricking the shopper
b. Snooping the shopper's computer

c. Sniffing the network
d. Guessing password
e. Stealing of user credentials or identity
f. Denial of service attacks
g. Using known bugs in the server, operating system or application software
h. Using server root exploits

There are measures that can be taken to overcome the negative impact of Malware. For example, individuals (representing consumer or citizens) can install personal firewalls and anti-Malware software in the computers that they use. Commercial organizations can deploy enterprise layered security defenses or security management services. However such measures are not holding up well against Malware attacks. In fact, there are reports claiming that majority of Malware attacks may have gone undetected [7]. It seems that the battle is still raging strong with no end in sight with the war being waged every day and perhaps every moment. One report by PC World advocates that the war may be working in favor of the Malware developers rather than the anti-Malware developers [8]. This paper reports a survey addressing the direct and indirect impact of Malware has on e-Businesses in order to arouse the awareness of the readers. This report also considers the impact of Malware on m-Commerce and Mobility computing. However the paper does not cover the intentions of these Malware attacks nor the forms of attacks launched on e-Businesses.

3. DIRECT IMPACT BY MALWARE

When a Malware attack is underway, its impact is significant and typically would have an immediate or near immediate reaction. To study the direct impact of Malware attacks, how the key e-Business actors are affected by such attacks are first considered. From records of past attack profiles, no e-Business actor has been exempted. Typically, the main intent of such direct attacks by Malware on the actors is to cripple its target's availability, to breach confidentiality (eg, stealing information) and/or undermine the integrity of its target.

3.1. Actor – End User

According to an AusCERT's survey [9], 23 percent of home computers are infected with Malware. Consumers using e-Business services are typically the prime targets of the Malware exploiters. For example, attacks on online banking are aimed at the customers of banks, with the intent to steal from these individuals rather than from bank's electronic vault [10]. A Microsoft staff, Danseglio, cited that the weakness link to Malware infection is human stupidity [11] that led to many successful social engineering attacks. To counter such assaults, good security practices are constantly advocated by organizations and governments to their constituents through education and reminders.

3.2. Actor – Commercial Organization

Malware has been used to launch Distributed Denial of Service (DDoS) attacks on organizations. Banks offering e-banking facilities to its customers are also targets of Malware attacks. Malware has further been advanced to attack the security defense mechanism put up by the banks. There are Malware designed specifically for a particular business. An example is the Banking Trojans which has been designed specifically to only harvest banking information from its infected targets [34]. Noticeably, the most popular form of attack done against commercial organizations is to disrupt the availability of business services offered online. However another form of attack is to defame the targeted. While organizations have established various forms of defenses like CAPTCHA (or Completely Automated Public Turing test to tell Computers and Humans Apart) which attempts to differentiate Malware from real customers, such countermeasures have been overcome [14]. Companies are responding by working together to combat Malware attacks. For example, eBay and Paypal are working with Google's webmail service, Gmail, to protect their customers from phishing attacks [15]. Others are looking to insure themselves with insurance from such Malware risks and its impact. A popular measure taken is to educate their end users with security advisories and good practices. All these are done to protect themselves, their customers and the relationships between them.

3.3. Actor – Intermediaries

Malware has attacked intermediaries which are services or infrastructure needed to fulfill e-Business activities. Such intermediaries include payment gateways, Certificate Authorities, Internet infrastructures like DNS, etc. The impact of an attack on any of these dependent intermediaries would have significant impact to e-Business activities. An example of such an attack is the DDoS attack in Dec 2008 on AlertPay.com which disrupted millions of businesses using this payment gateway service [16]. Service providers are responding to such assault. A broadband provider in Singapore, launched an 'Internet Clean Pipe' for banks that offers real-time monitoring, detection and protection to protect customers' online assets against DDoS attacks [17]. Another broadband provider in Israel offered Malware inspection on its inbound traffic to its customers. However according Huang et al [19], there are available technology solutions that can enable intermediaries to effectively mitigate the effects of a DDoS attack. However there is a lack of monetary motivation or business incentives for them to work collectively to mitigate such effects as compared to the targeted.

3.4. Actor – Critical Essential Infrastructure

Another major risk posed by Malware is attack against governments or organizations which has significant downstream impact to the actors of e-Business. An example is Malware attack on essential and critical infrastructure like power generation plants. In 2005, UK's National Infrastructure Security Co-ordination Centre (NISCC) reported that there had been a long-running series of attacks using targeted Trojans on companies that formed part of UK's critical national infrastructure like water and power [20]. In response, the UK government sent out security advisors to these companies of such critical infrastructure [35]. Another example of a proactive government response is by Australia's Critical Infrastructure Protection Branch, Attorney-General's Department [21]. Its plan is to increase its support to owners and operators of Australia's critical infrastructure to help the latter reduce the risks of electronic attacks. The support includes the following.

a. Studying espionage Malware undetectable by commercial anti-Malware solutions
b. Grants to be given to critical infrastructure owners and operators to conduct security assessments
c. Conduct domestic cyber-exercises
d. Establishment of business centre to facilitate sharing of security information between the government and critical infrastructure organizations to minimize security risks.

4. INDIRECT IMPACT BY MALWARE

Beyond the direct impact that Malware has made on e-Business, Malware has also induced other indirect or residual impact to its targeted actors and beyond. The impacts considered here are those that occur much later after the direct impact of Malware attack has been effected. Such impacts are typically reactionary.

4.1. Actor – End User

Information gathered or stolen by Malware attacks on e-Business actors are traded or sold online in e-Business channels. Beyond privacy, such information which belongs to end users can be further abused or exploited to cause more harm to these victims with subsequent malicious use. According to a survey by MessageLabs [3], most of the respondents stated that they lack confidence in traditional antivirus software. Also a number of the respondents said that the traditional antivirus will be obsolete within the decade. Fear of Malware or cyber crime has driven customers away from conducting online businesses. According to Salam et al. [23], the fear is quite significant. Some businesses have abused this fear by misleading their targeted customers to think that they have been infected by Malware and getting them to buy their anti-Malware solution to cure their 'infection' [24].

4.2. Actor – Commercial Organization

An important consideration in conducting e-Business is the relationship established between actors in order for the online e-Business transactions to occur. Customers are frustrated by the unavailability of e-services or slow performance resulting from the attacks of Malware. Such outcomes may result in customer attrition or reduction in e-Business transactions. Availability attacks on e-Business entities have resulted in permanent outage (demised) of the organization [26]. Interestingly Malware has some positive outcomes beyond the obvious like the creation of the ICT security industries especially in the area of anti-Malware solutions and products. Malware has been used to help increase sales of certain products. For example, consider Apple's advertisement that states its Mac OS X is not plagued with constant attacks from viruses and Malware [27].

4.3. Other Impact – The e-Business of Malware

Malware is sprouting its own online economy – the online shadow economy of Malware [28]. This new economy structure has established e-Business channels for Malware where Malware is the commodity being traded. The extent of advancement of this shadow's growth can be seen as the participants are behaving like the economies of 'legitimate' or 'good' ones. Malware authors are also dealing with copyright violations [29] and are turning to EULA [30] to protect their Intellectual Property. This economy even has its own supply chain where one would develop the Malware to exploit certain vulnerability, others to market the Malware 'solution', others to offer of professional services. Like other legitimate commercial product, prices of Malware drop with time [10]. According to an ITU study [31], the worldwide underground economy is estimated to be US$ 105 billion. Another interesting observation is the relationship that Malware propagation has with the world economy. According to a report by PandaLabs that when there is stock market drop, there is a spike in Malware circulation [32].

5. M-COMMERCE AND MOBILITY COMPUTING

The first Malware to hit the mobile platform, specifically the smartphones, occurred in 2004 [36]. By 2006, there were more than 300 kinds of Malware for this platform. Such malicious risk to mobility computing may also originate from convention computing platform like a standard PC. As mobility computing becomes more pervasive, it increases the urgency to protect Malware from the mobility platform and to m-Commerce intensifies.

Figure 1 – Malware 'Commwarrior.C' against Symbian OS (http://i.peperonity.com/)

In a research study done by Fleizach et al., it concluded that aggressive Malware in mobile networks could effectively launch denial-of-service attacks resulting in disruption to mobile services. This in turn may lead to unhappiness or losing confidence in using the mobility platform by customers, direct loss of revenue for m-Commerce retailers and intermediary service providers. The 2009 staff report [37] by Federal Trade Commission from United States of America advised its stakeholders to take precautions and develop strategies to mitigate possible effects of Malware in mobile commerce. It did acknowledge that Malware has not emerged as a significant problem as yet.

6. RESEARCH DIRECTION AND DISCUSSION

Malware's impact on e-Business is wide ranging. Hence there are many possible area of future research that can be carried out on Malware and e-Business. The effects of Malware notably go beyond the obvious (for example, unavailability of online services). Much like when a biological entity gets infected by a biological virus, the extent of harm caused by the infection is typically not localized. In many instances, the infection creates further complication to its infected host. The effects may go even beyond the biological realm into the psychological one. Similarly when Malware infects its target successfully and carries out its intended blow, is there any further repercussion beyond the obvious? Another area of research is how effective are current Malware counter measures and have such measures unintentionally affected the actors in a negative manner (for example, blacklisting legitimate entities)? More research can be done on Malware designed for a specific target within a specific industry and perhaps even within a specific locale like the Brazilian banking Trojans designed to attack Brazilian banks offering online banking [34]. Also more research is needed in the aspect of Malware attacks on the mobility computing platform.

7. CONCLUSIONS

In order for e-Business or e-commerce to flourish, online trust is vital. However it seems that Malware stands in the way of that intent. Malware is hurting the 'trust' factor vital to e-Business. Similarly Malware is a threat to the mobility computing platform and m-Commerce. However at the same time, Malware has started its own online business environment and is striving. There is now almost an economy evolving around Malware. More needs are required to develop effective counter measures to safe guard the general public's interest and the growth of e-Business.

REFERENCES

[1] T. Claburn, "Virus Found On Computer In Space Station", InformationWeek, Aug. 27, 2008. [Online]. Available: http://www.informationweek.com/news/security/antivirus/showArticle.jhtml?articleID=210201099. [Accessed Aug. 15, 2009].

[2] OECD Working Party on Information Security and Privacy (WPISP) in partnership with the Asia Pacific Economic Co-operation Telecommunication and Information Working Group (APEC TEL) Security and Prosperity Steering Group (SPSG), "Malicious Software (Malware): A Security Treat to the Internet Economy", OECD Ministerial Meeting on the Future of the Internet Economy., DSTI/ICCP/REG(2007)5/FINAL, Jun. 17, 2007.

[3] W. Sturgeon, "Fear of viruses and poor AV protection growing", ZDNet, Jul. 6, 2004. [Online]. Available: http://news.zdnet.com/2100-3513_22-137011.html. [Accessed Aug. 15, 2009].

[4] D. Khusial and R. McKegney, "e-Commerce security: Attacks and preventive strategies", Apr. 13, 2005. [Online]. Available: http://www.ibm.com/developerworks/websphere/library/techarticles/05. [Accessed Aug. 15, 2009].

[5] S. M. Poremba, "Majority of Malware attacks go undetected", SC Magazine, Aug. 11, 2008. [Online]. Available: http://www.scmagazineus.com/Majority-of-Malware-attacks-go-undetected/article/113673/. [Accessed Aug. 15, 2009].

[6] E. Larkin, "Malware Evolving Too Fast for Antivirus Apps", PC World, Dec. 31, 2007. [Online]. Available: http://www.pcworld.com/printable/article/id,140861/printable.htm. [Accessed Aug. 15, 2009].

[7] R. Gedda, "Home computers laced with Malware: survey", ComputerWorld, May 19, 2008. [Online]. Available:

http://www.computerworld.com.au/article/216531/home_computers_laced_malware_survey. [Accessed Aug. 15, 2009].

[8] S. Lawson, "Limbo Malware grabs personal banking data", ComputerWorld, Sep. 26, 2008. [Online]. Available: http://www.computerworld.com/s/article/9115721/Limbo_malware_grabs_personal_banking_data?taxonomyId=17&intsrc=kc_top&taxonomyName=security. [Accessed Aug. 15, 2009].

[9] R. Naraine, "Microsoft Says Recovery from Malware Becoming Impossible", eWeek, Apr. 4, 2006. [Online]. Available: http://www.eweek.com/c/a/Security/Microsoft-Says-Recovery-from-Malware-Becoming-Impossible/. [Accessed Aug. 15, 2009].

[10] S. J. Vaughan-Nichols, "How CAPTCHA got trashed", ComputerWorld, Jul. 15, 2008. [Online]. Available: http://www.computerworld.com.au/article/253015/how_captcha_got_trashed?fp=&fpid=. [Accessed Aug. 15, 2009].

[11] Internet Business Newsweekly, "eBay and PayPal Team up with Gmail to Fight Phishing", Internet Business Newsweekly, Jul. 21, 2008.

[12] D. Danchev, "AlertPay hit by a large scale DDoS attack", ZDNet, Dec. 1, 2008. [Online]. Available: http://blogs.zdnet.com/security/?p=2240. [Accessed Aug. 15, 2009].

[13] R. O. Storey, "Singapore's Starhub launches 'Internet Clean Pipe' for banks", MIS Asia, Dec. 11, 2008. [Online]. Available: http://www.mis-asia.com/news/articles/singapores-starhub-launches-internet-clean-pipe-for-banks. [Accessed Aug. 15, 2009].

[14] Y. Huang, X. Geng and A. B. Whinston, "Defeating DDoS Attacks by Fixing the Incentive Chain", ACM Transactions on Internet Technology, Vol. 7, No. 1, Article 5, Feb. 2007.

[15] M. Acey, "UK's critical infrastructure under Trojan attack", TechWorld, Jun. 16, 2005. [Online]. Available: http://news.techworld.com/security/3863/uks-critical-infrastructure-under-trojan-attack/. [Accessed Aug. 15, 2009].

[16] A. Yates, "National Security Briefing Notes: 2007 E-Security National Agenda", Australian Homeland Security Research Centre, Jul. 2007.

[17] A. F. Salam, H. R. Rao and C. C. Pegels, "Consumer-Perceived Risk in E-Commerce Transactions", Communications of the ACM, Vol. 46, No. 12, Dec. 2003.

[18] J. Leyden, "Ex-anti-virus chief in spyware scareware scam charges", The Register, Mar. 4, 2008. [Online]. Available: http://www.theregister.co.uk/2008/03/04/south_korea_scareware_fraud_charges/. [Accessed Aug. 15, 2009].

[19] T. Richardson, "Cloud Nine blown away, blames hack attack", The Reigster, Jan. 22, 2002. [Online]. Available: http://www.theregister.co.uk/2002/01/22/cloud_nine_blown_away_blames/. [Accessed Aug. 15, 2009].

[20] Apple Computers, "Why you'll love a Mac". [Online]. Available: http://www.apple.com/getamac/whymac/. [Accessed Aug. 15, 2009].

[21] M. Schipka, "The Online Shadow Economy: A Billion Dollar Market For Malware Authors", MessageLabs, 2007.

[22] L. O. Murchu, "Copyright Violations in the Underground", Apr. 25, 2008. [Online]. Available: http://www.symantec.com/connect/blogs/copyright-violations-underground#A97. [Accessed Aug. 15, 2009].

[23] J. Hruska, "Malware authors turn to EULAs to protect their work", ars technica, Apr. 28, 2008. [Online]. Available: http://arstechnica.com/security/news/2008/04/malware-authors-turn-to-eulas-to-protect-their-work.ars. [Accessed Aug. 15, 2009].

[24] ICT Applications and Cybersecurity Division, "ITU Study on the Financial Aspects of Network Security: Malware and Spam", ICT Applications and Cybersecurity Division, Policies and Strategies Department, ITU Telecommunication Development Sector, Jul. 2008.

[25] S. Gupta, "Cybercrime in 2009 - More Malware, More Difficult to Detect", Government Technology, Dec. 15, 2008.

[26] M. Ståhlberg, "The Trojan Money Spinner", Virus Bulletin Conference, September 2007. [Online]. Available: http://www.f-secure.com/weblog/archives/VB2007_TheTrojanMoneySpinner.pdf. [Accessed Aug. 15, 2009].

[27] National Infrastructure Security Co-ordination Centre, "NISCC Briefing 08/2005", National Infrastructure Security Co-ordination Centre, 2005.

[28] M. Hypponen, "Malware goes mobile", Scientific American, Nov. 2006.

[29] Office of Public Affairs, "FTC Issues Staff Report on Mobile Commerce Marketplace", Federal Trade Commission, USA, Apr. 22, 2009.

[30] C. Fleizach, M. Liljenstam, P. Johansson, G.M. Voelker and A. Méhes, "Can You Infect Me Now? Malware Propagation in Mobile Phone Networks", Workshop On Rapid Malcode, Proceedings of the 2007 ACM workshop on Recurring malcode, Pg, 61 – 68, 2007.