iS
CHANNEL

Risk Management and User Prevention for Malware Threats

Anand Paul
MSc Analysis, Design and Management of Information Systems
Information Systems and Innovation Group
Department of Management
London School of Economics and Political Science

KEYWORDS

Malware
Risk Management
Trojan
Zeus

ABSTRACT

Internet usage has been growing at a rapid pace over the last two decades. The crux of this paper is to highlight the attitudes of participation, motivation and educational awareness within risk management practices as a combined strategy for computer users, in home and in organizations, to suppress the growth of Malware in the internet. In the last decade, there has been a big growth in Malware spread on the internet and different forms of Malware continue to evolve. One such Malware is the 'Zeus Trojan'. It is found that Malware threat awareness and its damages provoke users to take notice of malicious activities on the internet and safeguard electronic data and assets. An industry outlook of the growth, evolution and spread of the Zeus Trojan Malware suggests that IS security should start from individual level and not with technology products.

Introduction

While the emergence of the World Wide Web has enabled unprecedented access to information, it has also created unprecedented opportunities to attack information assets (Galbreth and Shor 2010). Many computer users both at home and in organizations have become vulnerable to many malicious threats. "Given the pervasiveness of the personal computer, Internet use and the blurred line between work and home, IT security breaches on personal computers can cause damages not only to individuals but also to organizations" (Liang and Xue 2010: 395). One of the major IT threats within Information Systems is Malware. The OECD report describes Malware as "a general term for a piece of software inserted into an information system to cause harm to that system or other systems, or to subvert them for use other than that intended by their owners. Malware can gain remote access to an information system, record and send data from that system to a third party without the user's permission or knowledge, conceal that the information system has been compromised, disable security measures, damage the information system or otherwise affect the data and system integrity" (OECD 2009: 10). The web has been an arena for Malware activities that causes losses and negative consequences to those affected and IS professionals are very concerned about these malicious activities. A recent Q4 report published by McAfee (2010), a world leading security Technology Company, revealed Malware growth was going to be high in 2011 and also uncovered around 20 million new pieces of Malware in 2010 which equates to around 55,000 new Malware threats every day. One of these types of Malware is the 'Trojan horse'. This Malware seems to perform a useful function but also contains a hidden code that performs an unwanted malicious task without the user's knowledge. A deeper analysis of the types of Malware shows that the most prevalent Malware threats are Trojans - 59 % of all cases (Panda Security 2011).

A part of this paper explains about a growing Malware threat – the 'Zeus Trojan', a financial data steeling Malware, which has infected over 3.6 million computers in the United States (Binsalleeh, Omerod et al. 2010). This particular Malware has existed since 2007 and has evolved over time. A Symantec Security report (Falliere and Chien 2009) named 'Zeus' as the 'King of Bots' and a Trusteer (2009) report highlighted that 'Zeus' is probably the most painful financial Malware in the World Wide Web, both in terms of infection size and in terms of effectiveness. The latest reports tell that the Zeus Trojan has now attacked Blackberry and Android phones. In spite of these warnings, the 'Zeus Trojan' continues to infect computers all over the world. An alarming fact from research done by the security firm Trusteer (2009) Computers on a sample of 10,000 consumer computers in 2009 found that 55% of computers having updated Anti-virus were still Zeus infected. This infers that Anti-virus solutions have not excelled in their use and that Malware would continue to grow more complex. A complete dependence on only technol-

Corresponding Author
Email Address: a.paul3@lse.ac.uk (A. Paul)

ogy for defence from malicious threats might not be the way forward.

The remainder of the paper starts with an introduction to the Zeus Trojan Malware followed by available IS literature review. An incident relating to the Zeus Trojan and current evolution of this Malware in the industry allows author to discuss the importance of soft security. Finally the conclusions are listed.

The Zeus (Trojan Horse) Malware

One of the first incidents of the Trojan Horse can be traced back to early September 1986, when an intruder broke into a large number of computer systems in the San Francisco area, including nine universities, fifteen Silicon Valley companies, nine ARPANET (Advanced Research Project Agency Network) sites and three government laboratories and left behind recompiled login programs so that he could break into those same systems easier the next time (Reid 1987). The name 'Trojan Horse' "is inspired by the legendary wooden horse built by the Greek army, ostensibly as an offering to Athena, which in the dark of night disgorged its bellyful of murderous soldiers into the sleeping streets of Troy" (Denning 1990:288). Trojan horses require some level of user interaction to initiate the infection process such as clicking a web-link in an e-mail, opening an executable file attached to an e-mail or visiting a website where Malware is hosted (OECD 2009). Hence the author assumes that there is always an end-user involvement when Trojan Horses attack computer systems.

The Zeus is a Trojan Horse Malware that specializes in stealing banking credentials. The Zeus Trojan commonly infects computers via email phishing attacks or by 'drive-by-downloads', in which a Malware infects a user's computer without their knowledge when they visit a webpage (Cisco 2009). The Zeus Malware stays alert to know when a user logs into an account and then collects authentication credentials and passes the information to the hacker. Zeus has reportedly infected over 3.6 million computers in the United States (Binsalleeh et al. 2010). The Zeus Trojan is an easy toolkit that can create different versions of Zeus Malware. The program, when installed, connects to a command and control server where data is received from all Zeus infected computers (Stevens and Jackson 2010). The hackers then use this information to take over the user's accounts and transfer funds to a network of 'money mules' who are overseas individuals having bank accounts under fake identities. Once the money is received by the mules they transfer the cash back to the hackers and the mules are paid on a commission. Although this Malware was first identified in 2007, when it stole information from the United States Department of Transportation, it has not been possible to completely eradicate this IT threat. The latest reports of the Zeus Trojan is that the Malware is affecting smart phones- Symbian and Blackberry handsets and stealing online banking details (Wakefield 2011) showing that it has evolved.

Literature Review

"Enterprises establish computer security policies to ensure the security of information resources; however if employees and end-users of organisational information systems (IS) are not willing to follow security policy, then these efforts are in vain" (Herath and Rao 2009:106). The author's preferred way to prevent Malware is to start motivating end-users by involving them in security developments so that they would not only become aware of the current security threats they face but also they participate effectively in prevention of security incidents. The Protection Motivation Theory (PMT) (Rogers 1975) invokes a protective behaviour in end-users and might help to curb Malware incidents in the companies. This framework could be chosen because it has been successfully applied in many cases to understand the range of protective actions taken by individuals (Milne et al. 2000). The variables that capture PMT are perceived security to threat, probability of occurrence or vulnerability and efficacy of the recommended preventative behaviour. A lens into the Zeus Trojan Malware effect on these variables might help research to understand the applicability of the PMT theory on Malware.

In the OECD (2009) report, awareness is shown as an important line of defence against any forms of Malware. Public and private sectors have brought in awareness programmes to educate Internet users about Malware. Few examples of awareness programs include the Australian National E-security Awareness week, EU Safer Internet Plus Programme, UK government's Get Safe Online and United States Onguard Online. These programs would help the public to improve IS security at homes. Internet users at home could look for unusual symptoms on their computers such as strange screen graphics, unusual behaviour on reboot, unexpected sound effects, reduction in system performance and similar symptoms to involve themselves in the security measures. In case of organizations, computer training and education would protect the organizations because employees become more computer literate and protect organizational assets (Boss et al. 2009).

Another method of achieving awareness is by user participation (Spears and Barki 2010). There is a link seen between user-awareness and user participation. User participation raises organizational awareness of security risks and controls within business

processes that contributes to more effective security control development and performance (Spears and Barki 2010). User participation in IS security risk analysis and control design can provide needed business knowledge, thereby contributing towards effective security measures. "By taking a multi-approach combining different activities, hazards and disaster phases, participatory work is well placed to deal with the complexity of disasters and the diversity of factors affecting people's vulnerability" (Rudolph and Ahrens 2006:215). Also one can find that in organizations when end-users are involved in the development of security policies a feeling of closeness could be seen between the users and the organization which would also motivate employees to protect the organizational assets from the outside threats.

The author would like to suggest that the combined effect of user motivation (PMT), user awareness and user participation might prove to be a strong strategy to prevent the growth and evolution of Malware threats, such as the Zeus Trojan as explained through the case below.

Empirical case – A Zeus Trojan Incident

In June 2009, Jacques Erasmus and his research team at the security company Pervx discovered a list of File Transfer Protocol (FTP) credentials of accounts on domains that were high profile. The compromised accounts are linked to companies that include Bank of America, NASA, Monster, Oracle, Amazon and Cisco. These accounts were compromised by the Zeus Trojan which infected the victim's computers and then transferred the FTP credentials to a server located at a remote location. This Malware attack was discovered while the research team at Pervx was investigating a wild infection. The investigation followed the trail from the computer to the server where a dump file containing all the credentials was discovered. The report and the investigation details were passed on to the US-CERT (United States Computer Emergency Readiness Team) and companies were informed of this attack. The security company also created a list of domains so that companies can check if any of their employee's accounts have been attacked. The security company later provided instructions to clean up the infection on affected domains and suggested recommendations.

Continuing threat and evolution of the Zeus Trojan

The Zeus has continued to be a major Malware threat from 2007 and every year there are many incidents connected to the Zeus Trojan. In Feb 2011, William Hague, foreign secretary of UK, said that some computers in the British government had been infected with the 'Zeus' computer virus after users opened an e-mail ,claiming to come from the 'White House', and clicked on a link (BBC 2011). It is interesting to note that this Zeus Trojan has many different versions that have been created during the last few years and has evolved to an extent that updated Anti-virus solutions might not be able to detect the virus. A recent McAfee (2010) report has recently indicated that Zeus is also going moving towards mobile attacks. Cyber criminals know that many financial institutions use mobile SMS as a two-factor authentication method and therefore they are modifying the Zeus tool for starting similar attacks. From a prevention point of view, many anti-virus solutions are still ineffective on the Zeus Trojan. Security companies inform users that the Zeus Trojan cannot be detected by many technology products and provide step by step procedures to be followed thereby enhancing end-user participation and motivation from such Trojan attacks. One such example is given by Symantec, a security company that stresses end-users to exercise caution before opening e-mail messages and clicking URLs and not to fully rely on the Anti-virus solutions to prevent the Zeus Malware.

Discussion

Though the above Zeus Trojan incident has been stated and cited in many security journals and security websites, affected companies have not publicized this attack incident possibly due to reputation damage. However it is possible to presume to an extent on the risk management procedures or policies that have been changed because of such Malware attacks. Some of the traditional Information System Security (ISS) methods that are most commonly used include ISS checklists, ISS standards, Maturity Criteria, Risk Management and Formal methods (Siponen 2005). A critical analysis of these methods suggests that these methods are developed in isolation and that most of the traditional ISS methods are based on conceptual development offering little evidence to their usability and relevance in practice. All the affected companies in the Zeus Trojan incident would have been completely depending on technical solutions to prevent Malware attacks. After the incident, the author could now see an effort from the websites of few affected companies trying the educate end-users on the Malware threats which in turn enhances user participation to prevent Malware attacks to the systems. For example, Bank of America (2011) has a privacy and security site that educates users on the types of online fraud and protection techniques that involve user-involvement. Here, user-involvement activities include checking for the bank's trademark when logging into the website, ensuring that the address bar on the website turns green in colour, deletion of suspicious mails and even reporting suspicious mails to an e-mail address that handles such

suspicious mails. A look into the NASA (2010) website shows a new NASA Security Operations Centre (SOC) introduced in 2010 to fight Cyber-crime. The centre has brought about many awareness programs to educate end-users on types of cyber-crime and ways to prevent them. Meanwhile Cisco (2009) recommends that all web-users should erase any unsolicited request on the social networks as well as avoid clicking any applications or links in suspicious emails.

Threats such as the Zeus Trojan Malware which has the potential to cause major impacts on a global scale ought to be informed to the end-users. This would make the users aware and curious to know more about this dangerous Malware and the probability of occurrence in the Internet. Next, when the end-users understand that the Zeus Trojan has already caused financial damage in the world and updated Anti-virus solutions are unable to detect and remove this threat, there is further progress in motivation by increasing the perceived security to threat. Thirdly, many of the security companies have provided step by step procedures that require end-users to participate in the prevention of Zeus Malware attacks. These are treated as good practices when end-user encounters suspicious e-mails, unknown website links and illegal downloads and avoids them. If these steps are proved successful then end-users understand the efficacy of the recommended preventative behaviour. When all of the above points are placed together, these become the three factors that Protection Motivation theory is based on (Rogers 1975). Hence the author understands that the Protection Motivation Theory might be used to prevent such Malware incidents through user motivation and hopes future development of PMT theory to prevent Malware attacks.

Finally the author strengthens his stand that the latest security technology products cannot be completely dependent for removing Malware attacks. Hackers sometimes tend to attack those security packages that are rated high. Galbreth and Shor (2010) argues that adoption of a product by increasing the products market attracts more attackers. Hence there is also a danger if one over-relies on the latest technology products in the markets. An interesting point to think is whether security software companies add features in their products with adequate regard for the potential increase in vulnerability in a security product. This means that a technology product that can detect and remove Zeus version 2 might not be able to do the same for Zeus version 3. With competition among security companies for growth and market, a critical approach might be needed before adoption of technological products.

Conclusion

From the study it is seen that although technology products are used by individuals in organizations or in homes, information security cannot be achieved by completely relying on the technology products. A growing Malware threat in the Internet space – the Zeus Trojan is discussed through an incident and its evolution. Discussions around the study conclude that: a) a more user-involvement approach is needed to improve information security through a combined approach on participation, motivation and educational awareness. This approach is unique because many research papers discussed using either motivation or participation alone for better IS security but a combined effect could further strengthen the IS security. b) IS Security should start at the individual level where users would have to take more precautionary measures to prevent attack from evolving threats such as the Zeus and similar Malware. Safe security procedures or suggestions by Security industries are indicators about the necessity and strength of user participation and awareness to combat Malware. c) Many technology products lack strong detection and prevention techniques for many types of Malware and one is expected to shift from over-dependence on security technology products towards individual preventative actions. It is also seen that such security approaches might be cost-effective and sustainable for the future.

References

Albrechtsen, E. (2007) A qualitative study of user's view on information security. *Computers and Security*. 26(4) pp.276-289.

Bank of America (2011) Fraud Prevention and Identity Theft page for customer awareness. https://www.bankofamerica.com/privacy/Control.do?body=privacysecur_prevent_fraud (accessed 17 July 2011).

BBC (2011) William Hague: UK is under cyber-attack. http://www.bbc.co.uk/news/uk-12371056 (accessed 17 July 2011).

Binsalleeh, H., Ormerod, T., Boukhtouta, A., Sinha, P., Youssef, A., Debbabi M. and Wang, L. (2010) On the Analysis of the Zeus Botnet Crimeware Toolkit. *Eighth Annual Conference on Privacy, Security and Trust*. Ottawa, Canada.

Boodaei, M. (2011) Man-in-the-Browser attacks target the enterprise. Computerworld. http://news.idg.no/cw/art.cfm?id=7E66FDE5-1A64-6A71-CE16C4982827E112 (accessed 17 July 2011).

Boss, R.S, Kirch, J.L., Angermeier, I., Shingler, A.R. and Boss, W.R. (2009) If someone is watching, I'll do what I'm asked: mandatoriness, control, and information security. *European Journal of Information Systems*. 18(2) pp.151-164.

Bu, Z., Bueno,P. , Kashyap,R. and Wosotowsky,A. (2010) The New Era of Botnets. Santa Clara, McAfee Labs. http://www.mcafee.com/us/resources/white-papers/wp-new-era-of-botnets.pdf (accessed on 17 July 2011).

CISCO (2009) Annual security report. http://newsroom.cisco.com/dlls/2009/prod_120809.html (accessed 17 July 2011).

Denning, J.P (1990) Computer Viruses. In Denning, J.P (Ed.) *Computers under Attack: intruders, worms, and viruses* (pp.285-292). New York: ACM Press.

Dhillion, G., Silvia, L. and Backhouse, J. (2004) Computer Crime at CEFORMA: A case study. *International Journal of Information Management*. 24(6) pp.551-561.

Falliere, N. and Chien, E. (2009) Zeus: King of Bots. Cupertino, Symantec. http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/zeus_king_of_bots.pdf (accessed 17 July 2011).

Galbreth, R.M. and Shor, M. (2010) The Impact Of Malicious Agents On The Enterprise Software Industry. *MIS Quarterly*. 34(3) pp.595-612.

Hannan, M. and Tucker B. (2004) Risk Management and Organisational culture: The implications of Computer Network Attacks and Malware Incidents on Organizational Risk Management. *2nd Australian Information Security Management Conference*. Perth, Australia.

Herath,T. and Rao, R.H. (2009) Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems*. 18(2) pp.106-125.

Lee, Y. and Larsen, R.K. (2009) Threat or coping appraisal: determinants of SMB executives' decision to adopt anti-Malware software. *European Journal of Information Systems*. 18(2) pp.177-187.

Liang, H. and Xue, Y. (2010) Understanding Security Behaviors in Personal Computer Usage: A Threat Avoidance Perspective. *Journal of the Association for Information Systems*. 11(7) pp.394-413.

Liang, H. and Xue, Y. (2009) Avoidance of Information Technology Threats: A Theoretical Perspective. *MIS Quarterly*. 33(1) pp.71-90.

Loch, K. and Carr, H. (1992) Threats to Information Systems: Today's Reality, Yesterday's Understanding. *MIS Quarterly*. 16(2) pp.173-186.

McAfee (2010) McAfee Threats Report: Third Quarter 2010 shows Zeus attacking mobile. http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q3-2010.pdf (accessed 17 July 2011).

Milne, S., Sheeran, P. and Orbell, S. (2000) Prediction and intervention in health-related behaviour, a meta-analytic review of protection motivation theory. *Journal of Applied Social Psychology*. 10(1) pp.106-143.

NASA (2010) Security Operations centre for protection from Cyber Crime. http://www.nasa.gov/offices/ocio/ittalk/07-2010_soc_prt.htm (accessed 17 July 2011).

OECD (2009) Computer Viruses and Other Malicious software – A threat to the Internet Economy. http://www.keepeek.com/Digital-Asset-Management/oecd/science-and-technology/computer-viruses-and-other-malicious-software_9789264056510-en (accessed 17 July 2011).

Ollmann, G. (2008) The evolution of commercial Malware development kits and colour-by-numbers custom Malware. *Computer Fraud and Security*. 2008(9) pp.4-7.

Panda Security (2011) Trojans - Biggest Malware threat. http://press.pandasecurity.com/news/in-january-50-percent-of-computers-worldwide-were-infected-with-some-type-of-computer-threat/ (accessed 17 July 2011).

PNG, L.P.I. and Qiu-Hong, W. (2009) Information Security: Facilitating User Precautions Vis-à-vis Enforcement against Attackers. *Journal of Management Information Systems*. 26(2) pp.91-121.

PriceWaterhouseCoopers (2010) Information Security Breaches Survey 2010 - Technical Report. Report commissioned by Infosecurity Europe, London. http://www.infosec.co.uk/files/isbs_2010_technical_report_single_pages.pdf (accessed 17 July 2011).

Reid B. (1987) Viewpoint: Reflections on some recent wide spread computer breakins. *Communications of the ACM*. 30(2) pp.103-105.

Rogers, R. W. (1975) A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology*. 91(1) pp.93-114.

Rudolph, M.P. and Ahrens, J. (2006) The Importance of Governance in Risk Reduction and Disaster Management. *Journal of Contingencies and Crises Management*. 14(4) pp.207-220.

Siponen, T.M. (2005) An analysis of the traditional IS security approaches: implications for research and practice. *European Journal of Information Systems*. 14(3) pp.303-315.

Spears, L.J. and Barki, H. (2010) User Participation in Information Systems Security Risk Management. *MIS Quarterly*. 34(3) pp. 503-522.

Stevens, K. and Jackson, D. (2010) ZeuS Banking Trojan Report. Atlanta, DELL Secureworks. http://www.secureworks.com/research/threats/zeus/?threat=zeus (accessed 17 July 2011).

Trusteer (2009) Measuring the in-the-wild effectiveness of Antivirus against Zeus. New York, Trusteer Report. http://www.trusteer.com/files/Zeus_and_Antivirus.pdf (accessed 17 July 2011).

Vroom, C. and Solms, v.R. (2004) Towards information security behavioural compliance. *Computers and Security*. 23(3) pp.191-198.

Wakefield J. (2011) How safe is your smartphone? London, BBC. http://www.bbc.co.uk/news/technology-12710763 (accessed 17 July 2011).

Whitman, E.M. (2003) Enemy at the Gate: Threats to Information Security. *Communications of the ACM*. 46(8) pp.91-95.