Usability of Internet Security Software

Have They Got it Right?

Patryk Szewczyk
secau – Security Research Centre
Edith Cowan University
Perth, Western Australia
p.szewczyk@ecu.edu.au

***Abstract*— Security software usability has been an ongoing issue for end-users. Whilst manufactures have focused on making computers and operating systems more usable, the same cannot be said for security software. Whilst the number of threats continues to escalate, end-users are left attempting to implement a security solution on their own. Previous research has shown that users are unaware of Internet threats and do not know where to start with mitigation. This paper demonstrates that in 2011, Internet Security Software is gradually becoming more usable, although there are key elements which still require improvements. This paper shows the strengths and weaknesses of current security software, and proposes a series of solutions that software vendors should consider in future releases.**

Keywords- Security software usability, Internet security, network security, security

I. INTRODUCTION *(HEADING 1)*

Cyber intelligence company Cyveillance undertook a malware detection study in 2010 of the top thirteen anti-virus vendors. The experiment discovered that detection and resolution required a considerable period of time. Over a two week period only ninety percent of new malware was detected [1]. As a result, there is a significant timeframe whereby end-users may be vulnerable before any remediation is available. Malware anti-forensics or anti-avoidance techniques could be slowing down vendors from detecting and releasing signature updates [2]. Vendors may also be overwhelmed with the three hundred percent surge (in 2009) of newly released malware specimens over twelve months according to ScanSafe [3].

Malware continues to evolve from previously destructive software, to modern monetary theft software [4]. With such a large influx of malware circulating the Internet, one may ask how home users or those with little understanding of computer or network security are managing this ongoing issue. Ignorance may be a big factor with some individuals associating monetary income with an increased probability of being targeted through malware [5]. End-users also believe that should they have a security based issue that their Internet Service Provider (ISP) will provide adequate support [5]. However, in 2010 it was identified that many ISP's do not employ staff with an adequate understanding and expertise in countering Internet based threats. Instead staff tend direct end-users to information found on the ISP website [6]. Unfortunately ISP websites provide very few solutions to protect end-users [7]. One prevalent recommendation offered by ISP staff is to install an Internet Security Suite application.

Internet access is no longer a luxury but rather a necessity on which people depend on - to undertake business and/or leisurely interests [8]. Subsequently the reliance on a stable network complimented by usable security software is highly desirable. Commercial anti-virus vendors have responded to this and resultantly developed Internet Security Suites. ZoneAlarm like many other Internet Security Suite competitors, claim to provide; traditional PC based security, identity theft protection, browser security, and most importantly – a user friendly interface "Easy for anyone to use and customize" [9]. With marketing terms inclusive of "Extreme Security", "Titanium Internet Security", "360 Security", end-users may be lead to believe that by simply installing the product, safety would be guaranteed. Whilst end-users may be becoming vaguely more familiar with the concept of computer viruses [5], phishing scams for instance are still successful, even amongst age groups which have grown up utilizing the Internet [10].

Numerous reasons have been brought forward claiming why end-users become susceptible to phishing scams. End-users often judge legitimate websites by its aesthetics, security indicators are often un-trusted or misunderstood, awareness of scams and resultant consequences do not necessarily alter behavior [10]. These reasons indicate that end-users would benefit from usable software that explains threats and security concepts in layman terms. If security alerts are unnoticed, then the alerts would need to be presented in a manner that guarantees end-user interaction guided by step-by-step instructions. In 2009 a series of Internet Security Suites were analyzed against pre-defined Human Computer Interaction criteria. Researchers found that the usability of 2009 security software was inadequate. The complicated software interface and notifications coupled with an end-users lack of knowledge were found to be the main contributing factors [11].

The usability of security software has been a long standing issue. In 1975 it was identified that end-users would fail to adopt security systems unless they were easy to use [12]. In the paper "Why Johnny Can't Encrypt" [13] the researchers identified that with a well designed interface, participants in their study were still unable to use the software effectively. This study was further repeated in "Why Johnny Still Can't Encrypt" [14], and although the study was undertaken almost a

978-1-4577-0460-4/11/$26.00 ©2011 IEEE

decade later, similar issues arose. The ongoing issue rests on manufactures developing security software for experts by failing to understand what novice users require for software to be considered usable.

II. TESTING FOR USABILITY

ZoneAlarm has specifically set out to develop products aimed at novice end-users with design principles including; knowing and thinking like the target audience, eliminating product clutter and complexity, and minimising ineffective feedback to the user [15]. This paper resultantly compares and contrasts the usability of ZoneAlarm to its competitors. This will determine if the software has in fact been designed in a manner that as ZoneAlarm's Product Manager Jordy Berson claims – even his parents could utilise [15].

There is a fine line between making security software usable and weakening the overall strength of the solution. Security software must be planned and developed specifically for a target audience. Skilled computer users may use freely available firewalls, anti-virus, and anti-phishing software. However, novice end-users may trust the security software that vendors advertise through print, television and online media, or that comes pre-installed on a newly purchased computer. As a result Internet Security Suites should be developed to suit their intended audience – novice users'.

Whitten and Tygar [13] proposed a set of criteria governing what makes security usable. These criterions have been adopted and used in numerous research projects [16, 17]. The existing criteria were amended to be more relevant in evaluating Internet Security Suites. In this study the security software can be considered usable if the target audience;

- Is effectively informed why a threat is dangerous.
- Is provided with sufficient information and instruction to mitigate the identified threat.
- Is prevented from making destructive mistakes.
- Is not deterred from using the software persistently.

Criteria 1 is set on the foundation that any threat that the security software identifies should avoid specialized security language and explain the potential outcome if the subsequent attack were to be successful. Criteria 2 outlines that a user should be given simple guidance on the method by which to stop the current threat. Criteria 3 outlines that any action undertaken by the end-user should not be finite, and that any action can be undone, in a simple and quick manner. Criteria 4 outlines that the security software should behave passively, without continually interacting with the user.

The four aforementioned criteria are applied to ten 2011 Internet Security Suites. In contrast to only viewing the notifications of resultant NMAP scans [11], the experiment analyzed the notifications and prompts associated with; a series of vulnerability network scans, an attempt to download and install malware, and viewing of phishing websites.

The experimental procedure was centred on the Windows 7 Professional operating system. Ten Internet Security Suites were selected from a software reviewing portal [18]. These trial versions are listed in Table I. Each Internet Security Suite was respectively installed on a workstation utilising its default and/or (vendor) recommended configuration options.

To examine the usability of the security software a series of tests were performed to prompt the software to react. Vulnerability network scans were conducted utilizing Nessus 4 [19] prompting the end-user of a precursor to an attack [20]. Phishing websites [21, 22] were selected from PhishTank [23], mimicking PayPal scams and a fake anti-virus installer (TR/FakeAV.afr.1) [24] was used from Offensive Computing.

The experiment was undertaken by imaging Windows 7 on the target workstation with all Microsoft system and security updates applied upto April 10th, 2011. Each Internet Security Suite was installed independently utilising the default and recommended configuration suggested by the vendor. This was chosen to resemble an install strategy applied by a novice user. Nessus was utilised to undertake a subsequent scan of the victim machine, triggering the firewall to respond to port scans. The workstation was then used to access the phishing websites, and download/install the malware specimen. During each of the tests, empirical observations were made of the prompts or notifications provided via the Internet Security Suite according to the four criterions selected for the study.

III. USABLE SECURITY SOFTWARE

In contrast to previous studies [11] alerts from network vulnerability scans were only generated by Webroot and ZoneAlarm. This could be interpreted as a positive aspect where end-users are not bombarded with messages signifying little danger, yet a potential nuisance and product deterrent. Previously [11] Webroot raised alerts notifying the user that the firewall had detected a potential intrusion, without any further user interaction available. Such an alert may confuse a user and provide little guidance as to what to do next. ZoneAlarm appeared to be the market leader in terms of incident detection and usability – clearly conforming to its design goals. The results from the experiment will be analyzed against each of the four criteria identified previously.

A. Criteria 1

A prevalent issue raised among Internet Security Suite notifications was the chosen vocabulary the vendors have utilized. Whilst television and print media may make use of words such as 'virus' or 'website', some vendors have opted to replace colloquialism for technical words such as 'malware' or 'IP address'. This may still inform the end-user, but may not be as effective.

Should an end-user visit a phishing website, rather than immediately block the source, the program should educate the user as to why the site is dangerous. ZoneAlarm, BitDefender, Norton, eScan, Webroot and AVG detected the phishing websites and notified the user of the potential danger. The remaining five products even though they clearly state that they incorporate anti-phishing protection mechanisms – did not actually provide any protection or information regarding the potential threat. Subsequently, the researcher was permitted to navigate through each of the phishing sites without any consequence. Upon closer examination, it was noted that

Kaspersky was in fact aware of the potential phishing site. In the bottom right hand corner of the experimental workstation, a small notification was displayed informing the user that the site could be dangerous.

Figure 1. ZoneAlarm Phishing Website Warning

There is little merit from the end-users perspective, for security software to block access to a website, without any justification. If a potential threat be detected, it would seem appropriate for the security product to provide a brief outline of why the website has been blocked. As shown in Fig. 1 when the phishing website was accessed, ZoneAlarm blocked immediate access and presented the user with a warning. Keeping in line with criteria 1, the warning utilizes the technical term "phishing site", but then goes on to further educate and inform the user as to what a phishing site is. AVG utilized a similar concept whereby, a definition is provided as to what phishing is, but took one step further in providing hypothetical outcomes if the site is accessed and used.

Kaspersky raised a notification on the bottom of the browser stating "dangerous URL". It did not provide any further information, or explain what a URL is. Alternatively eScan blocked the website with text stating "Access Denied" followed by "Suspected Phishing Site", without a definition of possible consequences. In a similar manner Bit Defender presented the user with "The webpage has been blocked" because it "included objects that were infected", providing little information as to what an object is within the context.

In all but one instance, the malware specimen could be downloaded to the test workstation. Whilst ZoneAlarm informs users adequately of phishing sites, in the instance of malware it stated that the file downloaded "might be dangerous" as the "file is unsigned".

Trend Micro on the other hand didn't inform that a malicious file had been downloaded. Instead it took immediate action to remove the file after it had been downloaded and subsequently inform the user that "some security threats have been removed". The most interesting notification presented to the user was that of EScan. In this instance a pop-up window was presented informing the user of a file on the computer that is infected with a virus. The alert stated that this was a "dangerous situation" and that a scan should be conducted. Unfortunately, the pop-up had a four second count down before it would close, after which no further notifications would be displayed regarding the previous threat.

B. Criteria 2

It is vital that end-users are informed of threats in a manner which can be understood by all audiences. The subsequent actions following a threat alert can mean the difference mitigation or endangerment. The results from this experiment show that many Internet Security Suites do not provide sufficient information or instruction to mitigate the threat. One element in particular which would be beneficial to novice users is recommendations. Specifically, a user can be recommended to carry out a particular task should there be a threat. Few vendors incorporated this into their notifications.

ZoneAlarm provided a series of instructions which could be easily interpreted by any given audience. As per Fig. 1 after a user has been informed of the potential phishing website, they are then given two choices, one of which is recommended – to go back, and one which is not recommended – to stay on the site. Symantec's Norton 360 and AVG make clear recommendations informing that the phishing sites are malicious and that the user should not continue, but with an option available to continue should they wish to do so. Webroot and Trend Micro adhered to criteria 2, by advising of the potential dangers and making the ideal or recommended option larger and thus more noticeable than the "proceed to site" option which was small, and acting as a deterrent.

The remaining five security products did not provide sufficient information to the end-user, to effectively allow an individual to self mitigate the threat of phishing. For instance eScan completely blocks the phishing site and suggests that the "Systems Administrator" is contacted if access is required, or if the site is legitimate. One would have to question who an end-user would contact if the program suggests that an administrator needs to be contacted. Bit Defender blocks the website, and provides no instructions on how to unblock the site if it were safe. Interestingly the programs that did not explicitly alert the presence of a phishing website, did log the threat within the software itself, which is presumably of no use from a usability perspective to a novice computer user.

The guidance provided with relation to dealing with malware appears to be an overlooked task by vendors. Bit Defender, Eset, and Norton, block access to the malware specimen residing on the desktop. In this instance, no explanation was provided as to why the file was inaccessible; instead an alert was raised informing users of a virus. Norton in particular would not permit the file to be deleted. In every instance that an attempt was made to delete the file, Norton would alert that a threat was present, and that file was inaccessible. However, once a system virus scan was initiated, the file was removed. This does however; provide very little guidance for a novice user as to how to resolve such an event.

One of the prevalent outcomes of the experiment was the discovery of how little control a user has once a workstation is presumably infected with malware. Whilst, alerts are generated notifying of the threat, the user is predominantly instructed to click through a series of acceptances to initiate a scan or to agree in removing the malware specimen. Trend Micro, and ZoneAlarm did raise an alert of a potential virus when accessing the website containing the malware specimen. This fortunately did permit the user to agree or disagree in

downloading the potential threat to their system. Whilst an explanation of the threat was raised, no recommendations were generated as to whether or not the user should continue with the download or omit it entirely.

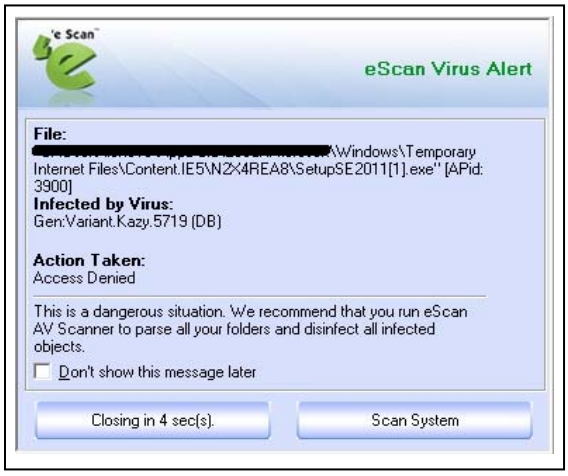

Figure 2. eScan Virus Alert Notification

C. *Criteria 3*

For an end-user to be prevented from making a destructive mistake, the security software would need to encompass a method by which to educate on the process to undo any action. For instance if a user is prompted to scan a file or system, and chooses to ignore or close the notification, there should still be a streamlined manner by which to undo or action the process. Unfortunately, none of the Internet Security Suites tested, encompassed a feature by which to prevent user mistakes.

Webroot was the only Internet Security Suite that requested permission from the user when a third party – trusted process was attempting to access the Internet (namely putty). In this instance, the prompt clearly detailed that an application was attempting to access the network, and requested that it either be allowed or blocked. The "remember this setting" checkbox was pre-selected, and a thirty second count down timer would automatically block the application from accessing the Internet. After the time frame was exceeded and the application was subsequently blocked, there was no clear method or instructions by which to undo this process. Had the firewall blocked an anti-virus program from accessing the Internet, this may have resulted in updates being denied.

D. *Criteria 4*

One of the surprisingly beneficial aspects of each of the Internet Security Suites was that all products passively secured the workstation. The products displayed alerts notifying that the trial period was soon to expire, although did not deter from its use. In each instance, the software would automatically update without user interaction.

E. *Criteria Summary*

Table 1 summarizes the results from this experimental study. The table displays the Internet Security Suites weighed against the pre-developed criterions. For each element the character *V, P or M* is used reflective of the network scan, phishing attack or malware. If the Internet Security Suite software did not effectively meet the criteria for each of the threats, then no resultant character is presented in the table.

As shown in Table I, effectively informing a user of the threat (criteria 1) is not undertaken appropriately. Should a threat be detected (phishing or malware) the security software should adequately explain what the threat is, and how this may affect the user. Not only would this act as awareness and educational technique, but it may also allow end-users to decide for themselves how to mitigate the subsequent threat. As presented in Table 1, it is clear that vendors do not wish to adequately guide a user to make an effective decision regarding a threat. Four of the ten Internet Security Suites provided no guidance as to how the user should deal with the threat that has arisen. As a result, an end-user may need to decide for themselves' what approach would be most suitable for the dilemma faced. If for instance the user is utilizing ESET, not only would instructions for mitigating the threat be omitted, but any information relating to the threat and potential outcomes is also not provided.

The predominant factor raised from this study is the elements relating to criteria 3. If consumers are overwhelmed with hypermedia based websites, then many security alerts may not be detected or noticed. As a result a novice user may inadvertently select the wrong option or omit a prompt as it is displayed for the security software. As a result, vendors must incorporate methods by which end-users may simply and easily revert a change made to the software as this may adversely affect and endanger their Internet experience. Criteria 1 and 2 could be improved through a toggle function – similar to what is implemented on many personal firewalls. This could be used to change the guidance and notification level provided by the software.

TABLE I. INTERNET SECURITY SUITE EVALUATION

Internet Security Suites	Criteria #1	Criteria #2	Criteria #3	Criteria #4
AVG Internet Security		P		VPM
Bit Defender Internet Security	P	M		VPM
Bullguard Internet Security	M			VPM
eScan Internet Security Suite	PM			VPM
ESET Smart Security				VPM
Kaspersky Internet Security	M			VPM
Norton Internet Security	P	P		VPM
Trend Micro Titantium Security	M	PM		VPM
Webroot Internet Security	PM	PM		VPM
ZoneAlarm Internet Security	VPM	PM		VPM
V = Vulnerability Scan, P = Phishing, M = Malware				

IV. CONCLUSION

This paper examined the usability of 2011 Internet Security Suites. The four selected criterions are highly suitable for evaluating the usability of security software as it covers four crucial elements. Two vendors specifically Webroot and ZoneAlarm appear to be leading the way in developing usable security software. This coincides with Webroot being rated as the top Internet Security Suite in 2011 [18] and ZoneAlarm's mission statement [15]. Unfortunately, there are still many vendors such as ESET and AVG who are not prioritizing the development of usable software for consumers. This would be suitable if the product was predominantly aimed at experts in the field who already have an in-depth understanding of such security products. However, AVG and ESET do market their products are being highly usable and use marketing techniques which make the product appeal to novice computing users.

To further validate the usability outcomes of this paper, current research in progress is evaluating the ten 2011 Internet Security Suites to a self proclaimed novice and expert audience. This will further validate the criteria utilized and the subsequent results generated. Whilst some of the Internet Security Suites appear to be usable, the same cannot be said for all security features currently available in software. As a result it is vitally important that vendors immediately focus on developing usable products, as this could easily attract additional customers rather than utilizing a series of marketing techniques. Specifically, the flawed area is interpretable notifications which are understood by a range of audiences. Vendors must realize that developing a unusable product may not only render the overall security product redundant, but may also deter the customer from renewing or purchasing the product in the future. With so many options available in today's market, there is little incentive for a novice user to continually utilize a usable product.

REFERENCES

[1] Cyveillance. (2010, April 5). Malware Detection Rates for Leading Malware Solutions. Available: http://www.cyveillance.com/web/docs/WP_MalwareDetectionRates.pdf

[2] M. Brand, C. Valli, and A. Woodward, "Malware Forensics: Discovery of the Intent of Deception," Journal of Digital Forensics, Security and Law, vol. 5, pp. 31-42, 2010.

[3] ScanSafe. (2009, December 11). ScanSafe Annual Global Threat Report 2008. Available: http://www.scansafe.com/downloads/gtr/2008_AGTR.pdf

[4] G. Cluley, "Sizing up the malware threat – key malware trends for 2010," Network Security, vol. 2010, pp. 8-10, 2010.

[5] P. Szewczyk and S. Furnell, "Assessing the online security awareness of Australian Internet users," in 8th Annual Security Conference, Las Vegas, NV, 2009.

[6] P. Szewczyk and C. Valli, "Ignorant Experts: Computer and Network Security Support from Internet Service Providers," in 4th International Conference on Network and System Security, Crown Conference Centre Melbourne, Victoria, 2010.

[7] P. Szewczyk, "Security Information Supplied by Australian Internet Service Providers," in 8th Australian Information Security Management Conference, Duxton Hotel, Perth, Western Australia, 2010.

[8] E. Kritzinger and S. H. v. Solms, "Cyber security for home users: A new way of protection through awareness enforcement," Computers & Security, vol. 29, pp. 840-847, 2010.

[9] CheckPoint. (2011, April 20). ZoneAlarm Internet Security Suite. Available: http://www.zonealarm.com/security/en-us/zonealarm-computer-security-suite.htm

[10] S. Sheng, M. Holbrook, P. Kumaraguru, L. F. Cranor, and J. Downs, "Who falls for phish?: a demographic analysis of phishing susceptibility and effectiveness of interventions," in 28th International Conference on Human Factors in Computing Systems, Atlanta, GA, USA, 2010.

[11] T. Ibrahim, S. Furnell, M. Papadaki, and N. Clarke, "Assessing the Usability of End-User Security Software," in 7th International Conference on Trust, Privacy & Security in Digital Business, University of Deusto, Bilbao, Spain, 2010.

[12] J. H. Saltzer and M. D. Schroeder, "The Protection of Information in Computer Systems," Proceedings of the IEEE, vol. 63, pp. 1278-1308, 1975.

[13] A. Whitten and J. D. Tygar, "Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0," in 8th USENIX Security Symposium, Washington, D.C., 1999.

[14] S. Shang, L. Broderick, C. A. Koranda, and J. J. Hyland, "Why Johnny Still Can't Encrypt: Evaluating the Usability of Email Encryption Software," in Symposium on Usable Privacy and Security, Carnegie Mellon University, Pittsburgh, PA, 2006.

[15] J. Berson, "ZoneAlarm: Creating Usable Security Products for Consumers," in Security and Usability: Designing Security Systems That People Can Use, L. F. Cranor and S. Garfinkel, Eds., ed North Sebastopol, CA: O'Reilly Media, 2005.

[16] A. Beautement, M. A. Sasse, and M. Wonham, "The compliance budget: Managing security behaviour in organisations," in 2008 Workshop on New Security Paradigms, Colonial Inn, Concord, MA, USA, 2008.

[17] J. Goecks and W. K. Edwards, "Challenges in Supporting End-User Privacy and Security Management with Social Navigation," in 5th Symposium on Usable Privacy and Security, Mountain View, CA, USA, 2009.

[18] TopTenReviews. (2011, March 10). Internet Security Suites Software Review. Available: http://internet-security-suite-review.toptenreviews.com/

[19] Tenable. (2011, March 11). Tenable Network Security. Available: http://www.nessus.org/products/nessus

[20] S. Jung, J. H. Kim, G. Gagalaban, J.-h. Lim, and S. Kim, "Design of Cyber Attack Precursor Symptom Detection Algorithm through System Base Behavior Analysis and Memory Monitoring," Communications in Computer and Information Science, vol. 2010, pp. 276-283, 2010.

[21] (2011, April 20). Available: http://paypal.hostpo.net

[22] (2011, April 20). Available: http://vk-quests.info

[23] OpenDNS. (2011, April 25). PhishTank: John the fight against phishing. Available: http://www.phishtank.com/

[24] (Security Essentials 2011, April 20). 2011. Available: http://se-get-11.com/SetupSE2011.exe