2006

The Awareness and Perception of Spyware amongst Home PC Computer Users

M Jaeger
University of Plymouth

N L. Clarke
University of Plymouth

DOI: 10.4225/75/57a80d64aa0ca
Originally published in the Proceedings of 7th Australian Information Warfare and Security Conference, Edith Cowan University, Perth Western Australia, 4th - 5th December, 2006.

The Awareness and Perception of Spyware amongst Home PC Computer Users

M. Jaeger and N.L. Clarke

Network Research Group, University of Plymouth, Plymouth, UK
e-mail: nclarke@plymouth.ac.uk

Abstract

Spyware is a major threat to personal computer based data confidentiality, with criminal elements utilising it as a positive moneymaking device by theft of personal data from security unconscious home internet users. This paper examines the level of understanding and awareness of home computer users to Spyware. An anonymous survey was distributed via email invitation with 205 completed surveys. From an analysis of the survey it was found that the majority of respondents do understand what Spyware is, however, there was found to be a lack of understanding of computer security in defending against Spyware, with 20% of survey respondents not using any Anti-Spyware. In addition, the subjective nature of survey respondent's ideas of Spyware infected websites was established and compared to past web-crawl research where a high proportion of survey respondent's opinions were found to be incorrect. It was also found respondents see Spyware as a 'High/Some Threat', and due to past infections and news/media articles 72% have changed their browsing habits.

Keywords

Spyware, Anti-Spyware Software, Spyware Web-Crawl, Information Security

INTRODUCTION

In recent years there has been an emergence of software known as Spyware, programs created both for the covert and overt acquisition of personal or non-personal information from a personal computer (PC) connected to the internet (Sariou et al., 2004). This is now a persistent security problem to home PC users; the old security culprits of Malware (viruses, worms etc), are being superseded by Spyware, and to a lesser extent other newer forms of Malware e.g. key loggers and email phishing. Spyware programs are able to hide via changing their signature, execute code without user intervention and move through networks invisibly whilst serving their own purpose.

Most research undertaken on Spyware is based on levels of Spyware infection on scanned desktop PC's, for example a survey by National Cyber Security Alliance (NCSA) in 2005 found from 354 respondents 38% had no Spyware protection, yet 83% felt safe from online threats; however 61% of the respondents had a form of Spyware or Adware on their PC. Equally an analysis report on Spyware from Webroot Software Inc (2005) stated that during the course of the third quarter of 2005, an important and alarming Spyware trend emerged, where many home computer users are admittedly afraid of becoming a victim of identity theft from using the Internet. So some home PC users are worried and others are not.

This research aims to use past research into Spyware and infected website categories to ask home PC users which websites they think are the most likely to have Spyware. Original questions were asked of survey respondents, for example do respondents use Anti-Spyware and if so what vendor, do they understand what Spyware is and what level of threat do they feel from Spyware; respondents were also asked if they had changed their internet browsing habits due to past infections and or world news media articles. This papers format is to outline past Spyware research, followed by the methodology to investigate the attitudes of home PC users to Spyware. Specific aspects of research will be looked at; in terms of understanding what Spyware is, the use of Anti-

Spyware software and the subjective belief of Spyware infestation in specified website categories. These results are then discussed and conclusions presented.

BACKGROUND

Most research on Spyware has been completed on the identification, categorisation and removal of Spyware; this new research looks at Spyware from the subjective viewpoint of the home PC user, as well as security measures employed. Past research has made little effort into understanding user awareness of Spyware and its activities; however some good research has been conducted.

This is shown by work produced by Freeman and Urbaczewski (2005) which states reasons why people hate Spyware. A paper by Zhang (2005) shows consumer understanding of Spyware in terms of their knowledge level. This is again revealed by a similar study by Qing and Tamara (2005), who believe in the concept of educating PC users to remove complacency that they have over Spyware, this research established user awareness factors were most accurate in showing which users took active measures against Spyware. Whilst a research paper created by Awad and Fitzgerald (2005) took a different viewpoint looking at what consumers find most deceptive about Spyware. Even though home PC users are worried about internet identity theft they do seem to have a love-hate aspect to Spyware, consumers will allow its usage on their own home PCs if there is a pay off i.e. in terms of peer-2-peer (P2P) software where the ability to download anything they want is assuaged by Spyware monitoring what they are doing. These are seen as "Overt Providers" by Warkentin et al. (2005) and this research also points to creating new legislation to segment Spyware software into positive and negative forms, with legal protection for some and prosecution for others.

As Spyware becomes a more prevalent infection vector, more research needs to be undertaken into what home PC users actually think about Spyware in terms of their level of understanding, security implemented and awareness as to where they think Spyware is on the Internet. Current Spyware articles point to a major problem in consumer understanding of Spyware due to complacency, lack of knowledge or an inappropriate safe feeling whilst using the internet, consumers seem to have an 'it won't happen to me' attitude to Spyware infections.

METHODOLOGY

The method selected for this avenue of research was an online survey. The analysis of the survey data was via quantitative analysis; this analysis form was chosen as it shows a complete, detailed depiction of the collected data; whilst interpreting data distinctions by using logical human deductions. Creation of the survey was completed over a number of iterations to produce the correct syntax and structural flow. The survey was distributed over a five month period (03/2006 – 07/2006) and the data collection was anonymous, allowing for more candid question answering. Survey invitation was via the use of email (containing the survey web link and basic information about the research) and was distributed to a wide range of people including academia, business and home users.

Given the nature of the questionnaire it was decided to select the respondent's computer skill as a basis of comparison. Traditional demographic factors such as age, gender or education would not provide a reliable basis as computer knowledge and skill is independent of these factors. However, care has be taken in interrupting the results due to the subjective nature of under or overestimating ones own ability. Four categories of computer skill were created: Novice home PC user, Intermediate home PC user, Advanced home PC user and IT Professional. A skill set example was provided for each level, each level encompassed a series of computer skills which increased in knowledge and complexity dependent on the respondents understanding of computing. The survey was partitioned into 6 sections; grouping together similar avenues of questioning. The sections are as follows: PC Usage, PC Setup/Configuration, Experiences of and with Spyware, Understanding of Spyware, Past Spyware Infections and Other Known Internet Security Threats.

RESULTS

An analysis of respondents by their subjective assessment of computer skill (Table 1) highlights a fairly broad spectrum of users in each category, with the single exception of those classifying themselves as novice home PC users. Given the survey's method of execution via email it is anticipated that a far greater number of computer literate people would have responded to the survey. Given the skew towards more technically competent users, it is suggested that the results presented in this paper might reflect a slightly better perspective of Spyware and security than is experienced by the general population.

	Novice Home PC User	**Intermediate Home PC User**	**Advanced Home PC User**	**IT Professional**
Number of Respondents	1%	36%	37%	25%

Table 1: Breakdown of Respondents by Computer Literacy

An opening question was asked of the 205 survey respondents, 'what is your home computer used for' e.g. Email and Online Shopping; results are shown in Figure 1.

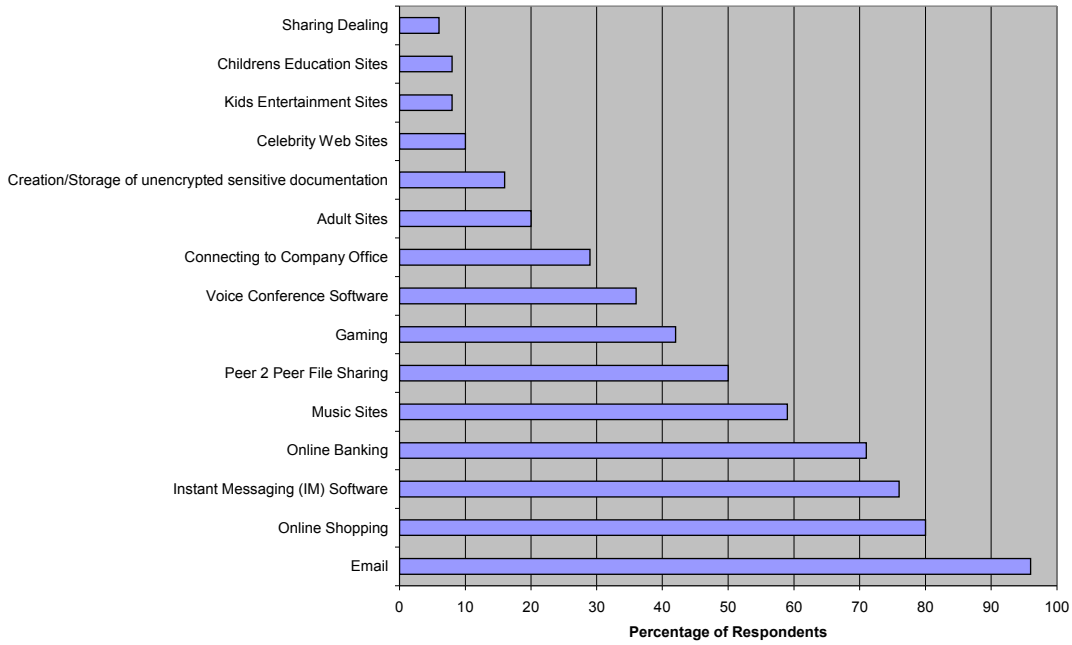

Figure 1: What Is Your Home Computer Used For?

An interesting piece of data from Figure 1 points to 50% of respondents using P2P software, P2P software is a known harbour for both Spyware and other forms of Malware. As such these respondents must be tacitly accepting possible infections as a consequence of the possible positive P2P software usage.

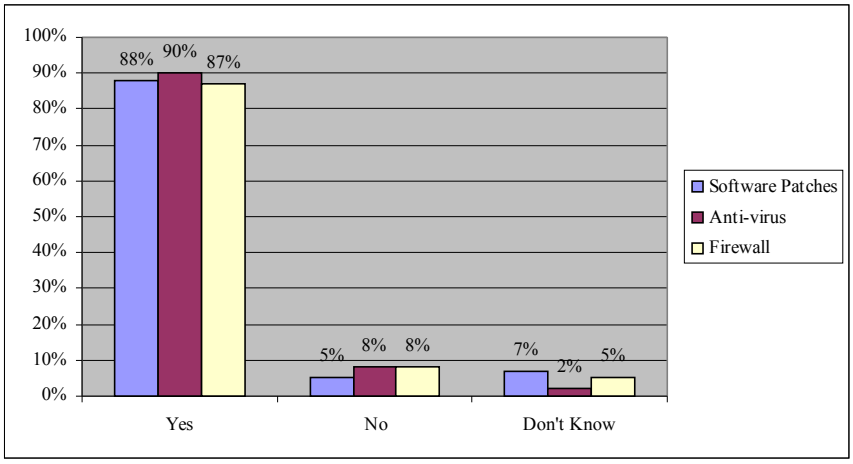

Figure 2: Percentage of Home Computer Users Using Anti-Virus, Firewalls and Software Patching.

This was followed by a question about whether they software patched their home computer, used a Firewall and used Anti-Virus software; these results are shown in Figure 2. What can be seen is that most respondents do use these security controls, however a small proportion do not, whilst some 'Don't Know' if they do or don't, this data can also be looked at alongside how many respondents use Anti-Spyware in Figure 3.

	Total	**Have you heard of (come across the phrase) "Spyware" before?**	
		Yes	**No**
Total	**205**	196	9
		96%	4%

Table 2: What Do You Feel Is Your Skill Level With Your Home PC?

Of the 196 respondents who had heard of Spyware, as shown in Table 2, only 82% of these respondents picked the most widely decided definition of what Spyware is (as shown in Table 3), that being 'Spyware gathers information about what I am looking at on the internet and sends it back to a central computer.'

	Total	**Novice Home PC User**	**Intermediate Home PC User**	**Advanced Home PC User**	**IT Pro**
Total	**196**	2	68	75	51
Spyware is a nasty computer virus.	9	1	7	1	0
		50%	10%	1%	0%
Spyware sends me to annoying web sites I don't want to go to.	7	0	4	1	2
		0%	6%	1%	4%
Spyware gathers information about what I am looking at on the internet and sends it back to a central computer.	161	1	44	70	46
		50%	65%	94%	90%
Spyware is a form of annoying popup advertising that appears when I go to certain web sites.	19	0	13	3	3
		0%	19%	4%	6%

Table 3: Which Phrase Best Describes What "Spyware" Could Be?

Conversely for the respondents that had heard of Spyware, Table 3 shows the survey data details. As such the user groups who understood what Spyware is were unsurprisingly the Advanced Users and IT Professionals; however there does seem to be some misunderstanding of what Spyware is. From the data 18% (35 respondents out of the 196 respondents that know what Spyware is) misidentified Spyware as either a 'Virus' – 9 respondents, or 'Adware' – 7 respondents, or finally a 'Pop-Up' – 19 respondents. Survey respondents in general do seem to know from this survey what Spyware is, as can be seen in Table 3, where 79% or 161 respondents out of the total of 205 respondents correctly knew what Spyware is.

	Total	**Removed it myself with my Home PC's Anti-Spyware software.**	**Required my home PC's customer support to help me remove Spyware using my home PC's Anti-Spyware software.**	**Called my home PC's customer support with problem, told to download Anti-Spyware, then walked through how to use it.**	**Unable to remove it from home PC, had to reinstall all software including operating system.**
Total	**196**	104	3	3	15
No, I have never had a "Spyware" infection.	71	0	0	0	0
		0%	0%	0%	0%
Yes, up to 3 Months ago.	65	54	2	3	6
		52%	67%	100%	40%
Yes, up to 6 Months ago.	16	14	0	0	2
		14%	0%	0%	13%
Yes, up to 9 Months ago.	8	6	0	0	2
		6%	0%	0%	13%
Yes, up to 1 year ago.	16	14	0	0	2
		14%	0%	0%	13%
Yes, 1+ year(s) ago.	20	16	1	0	3
		15%	33%	0%	20%

Table 4: Past Spyware Infections on Respondents Home PC's and Resolution Methods Used.

As can be seen from Table 4 of those who had heard of Spyware (as found in Table 2), a high proportion (64%) have had a Spyware infection, this is much more than those that have not had a Spyware infection. Of those that had acquired a Spyware infection most were able to remove the problem themselves, as shown by Table 4 where 53% of all survey respondents used their own Anti-Spyware to remove the infection from their PC. Only a small proportion (3%) required 3rd party customer support help. Furthermore, only 8% of survey respondents had to re-image their home computer.

In terms of defending themselves against Spyware, of the Anti-Spyware software used there is a clear winner as shown in Figure 3; furthermore it seems many consumers use multiple Anti-Spyware software, as the total of Anti-Spyware software used (215) is larger than the total survey response of 205. Spybot comes top with 36% of respondents using the software, its high usage is probably down to being freeware, as well as having been around the longest (since at least October 2002), it is also updated regularly and is known to have a good scan engine. Next is Lavasofts Ad-Aware, again this software has a freeware version that is regularly updated but has not been

around for as long as Spybot. Next is the 20% of respondents who don't use any Anti-Spyware software at all, this equates to 39 respondents; comparing this answer to survey security questions on Anti-Virus, Firewall usage and security patching we find the following respondents who do not use any Anti-Spyware software; where 13 respondents do not use Anti-Virus, 6 respondents do not use a Firewall and 3 respondents do not security patch the Operating System of their home PC. This information points to the glaring problem of why Spyware can spread quickly in this age of Broadband communications; the problem is that the onus is on the PC owner. With that comes a disparate level of computer security knowledge.

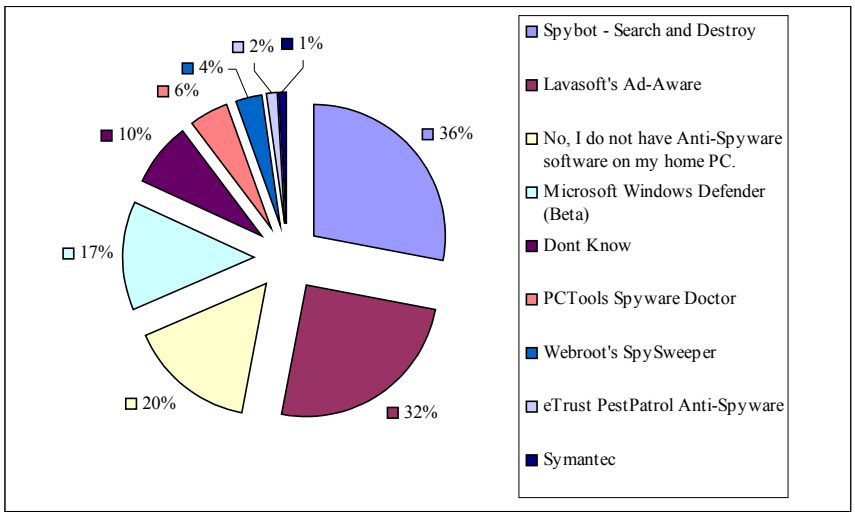

Figure 3: % Breakdown Of All Anti-Spyware Software Used On Each Respondents Home PC.

Subsequently, a question was asked in terms of the type of sites that could contain Spyware, the web site classifications covered most of the main sites people go to and the results can be seen in Table 5. From Table 5 it can be seen that Adult Oriented sites and Pirate Software site are what respondents think contain the most Spyware; with the least likely being Online News sites followed by Kids oriented websites.

	Definitely/Yes	**Possibly/Maybe**	**No**	**Don't Know**
Adult Entertainment	72%	24%	1%	3%
Pirate Software/Warez	70%	21%	3%	6%
Screensaver/Wallpaper	37%	42%	10%	10%
Music Orientated	23%	61%	8%	8%
Games Oriented	22%	60%	11%	7%
Celebrity Oriented	18%	61%	8%	13%
Kids Orientated	11%	43%	32%	14%
Online News	5%	33%	45%	17%

Table 5: Home PC Users Opinion of Website Categories That Contain Spyware.

In terms of other forms of Malware infections, respondents were asked if they had received a Phishing email, just under half of respondents - 48%, had received a phishing email trying to obtain personal data, whilst 52% had not. From this avenue of questioning respondents were also asked as to what other Malware infections/devices they had been infected by, these are seen in Figure 4.

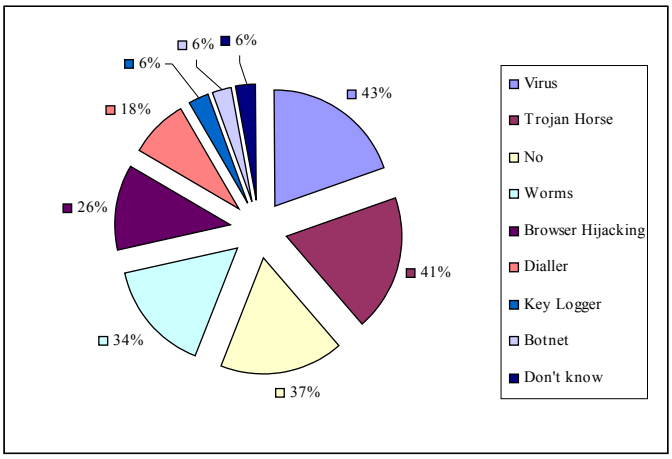

Figure 4: Other Malware Infections as % of Respondents.

What can be seen in Figure 4 is that the old sources of Malware infection are still evident: Viruses, Trojan Horses and Worms. Even as more recent forms of infection vector are becoming more plentiful. This can be seen by the level of Browser Hijacker, Key Logger and BotNet infection. Additionally Dialler infections will probably reduce over time as Broadband becomes the mainstream, with less narrowband internet connections used.

	High Threat	**Some Threat**	**Very little Threat**	**No Threat**	**Don't Know**
Virus	56%	35%	8%	1%	1%
Worm	54%	28%	11%	1%	6%
Trojan Horse	55%	26%	9%	3%	7%
BotNet	27%	26%	18%	5%	24%
Key Logger	37%	23%	17%	6%	17%
Dialler	21%	27%	20%	15%	17%
Browser Hijacking	26%	31%	21%	7%	14%
Email Phishing	31%	28%	20%	13%	8%
Spyware	35%	40%	17%	3%	5%

Table 6: Threat Levels As Seen By Survey Respondents.

The survey respondents were then asked as to how much of a threat Spyware was to them on a scale from 'High Threat' to 'No Threat', the results are seen from Table 6. As can be seen the highest response to Spyware by 40% of home PC users was as 'Some Threat', the next highest response was from 35% of respondents who saw Spyware as a 'High Threat'. This indicates that Spyware is seen as a threat by 75% of survey respondents.

On your home PC have you become more careful about what web sites you visit on the internet generally due to any of the below reasons?	
Yes, due to past infection/attack.	33%
Yes, due to information from 3rd party (e.g. TV News, Newspaper, etc.).	22%
Yes, due to past infection/attack and 3rd party information.	17%
No, I have not become more cautious.	28%

Table 7: Have You Changed Your Website Browsing Habits Due To A Specific Reason?

Furthermore, as can be seen from Table 7 a large proportion of the survey respondents have changed their website browsing habits, mainly due to past internet based infections and attacks i.e. Spyware. In total the respondents that changed their browsing pattern total is equal to 72% or 148 respondents.

DISCUSSION AND EVALUATION

The results have shown that almost all respondents understand correctly what Spyware is, and of all the respondents a healthy amount use Anti-Spyware. Though from past history a high proportion of home PC users have had a Spyware infection, more than double those that have not. Furthermore most of these past infected respondents were able to remove the Spyware themselves with little outside help. This indicates that Anti-Spyware is becoming easy to use and effective. What is also of interest is that though software is seemingly able to remove Spyware, consumers seem to be doubling up with one to two Anti-Spyware software programs. It seems they may not be totally confident in the software yet, this may be due to the recent creation of most Anti-Spyware e.g. Microsoft's Anti-Spyware software in January 2005. Only 39 respondents do not actively use Anti-Spyware, these respondents are not protected from Spyware and possibly will infect other people; they can be seen as a threat to the personal data security of others who do not use Anti-Spyware. However, Anti-Spyware users must keep their software regularly updated, as the Anti-Spyware users are only as well protected as their software is regularly updated.

The survey has highlighted the high proportion of respondents who use Peer to Peer (P2P) software (a known Spyware infection route). Does this mean that Spyware monitoring in P2P software is ok for some consumers, where this type of Spyware used is seen as an "overt provider" by Warkentin et al. (2005). Does this then mean as Warkentin et al. (2005) states that some consumers see some Spyware as ok, as long as they get some kind of positive benefit from losing some of their online privacy. If this is the case does this not mean that not all Spyware is as bad as we think? As Warkentin et al. (2005) state in their research, legislation does not sufficiently cover the differential nature of Spyware, and that a comprehensive categorisation of Spyware must be undertaken to produce a far more democratic legislation process. This is needed, as can be seen in the grey area of client/server management agents like SNMP being used on employee's corporate computers. The agent software could possibly be classed akin to Spyware dependent on how it is used, as the likelihood is the employee will not know about it, and that data may or may not be used remotely in the company by other departments.

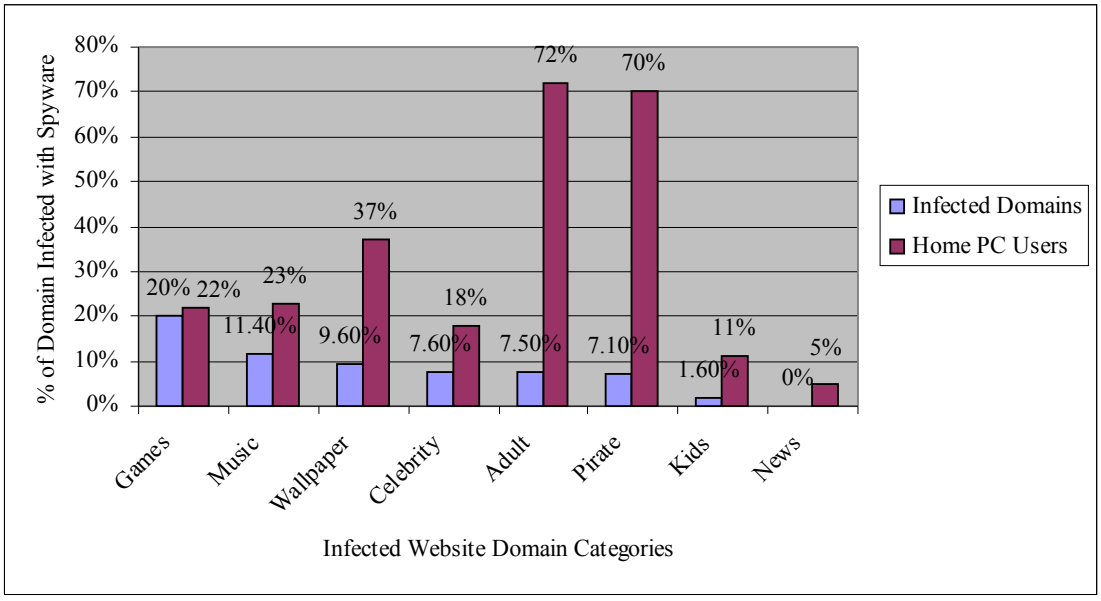

Figure 5: Executable Spyware Infections across Web Categories.

In terms of evaluating the subjective understanding of Spyware infested websites it can seen that what sites respondents believe are infected with Spyware differs from what research has shown to be sites that contain Spyware. Figure 5 compares the results found in Table 5 with research conducted by Moshchuk et al. (2006). Moshchuk et al. performed a web-crawl during 2005 across a number of website categories looking for Spyware. From the graphical extrapolation in Figure 5, the Top 4 website domains containing Spyware can be seen in descending order: Games websites (20%), Music websites (11.40%), Wallpaper/Screensaver websites (9.60%) and Celebrity websites (7.60%). From the survey results in Figure 5, the respondents understanding of which websites categories that contain the most Spyware can be gauged, with the following Top 4 website categories, in decreasing order have the most inherent Spyware: Adult Entertainment websites (72%), Pirate Software websites (70%), Wallpaper/Screensaver websites (37%) and Music Orientated websites (23%).

From this evaluation of respondent's subjective assumptions it can be safely said that survey respondents were wrong about the top 4 Spyware infested website categories. It is suggested that their assumptions are probably down to preconceived prejudices against certain website categories. Though respondents may not know where Spyware is, they do feel that it is a threat, as survey results point out that the majority of respondents see Spyware as a 'High/Some Threat'. This is a feasible reason why a high proportion of respondents have changed their internet browsing habits, as a consequence of primarily past infections/attacks from for example Spyware; and secondly, news/media articles on the threat of Spyware and the associated loss of personal data from their personal computer.

CONCLUSIONS

Even though it seems a high proportion of home PC users understand the need for security software i.e. Anti–Spyware, and information is being understood in terms of this threat, there is still a problem of low computer security knowledge in a proportion of respondents. As stated by both Qing and Tamara (2005) and Zhang (2005); it creates user reservations in doing anything about possible current or future Spyware infections. Conversely, some respondents use multiple Anti-Spyware software from different vendors, seemingly showing a current low level of trust in current software, with most only using one vendor, and a small proportion using none. However, the use of Anti-Spyware is moot unless it is kept up to date with scanning engine/signature patches. Nonetheless, most that have had a past infection were able to remove it themselves with their own Anti-Spyware. Those that needed 3rd party help were also able to remove their Spyware infection, and only a small proportion was unable to and had to re-image their PC. This end user ability points to current software being easy to use and effective against current Spyware. Furthermore a large proportion of respondents do seem to understand what Spyware is in terms of a current definition, whilst seeing Spyware as a 'High/Some Threat'. This correct understanding of Spyware is however at odds with their incorrect judgment of which website category's contain Spyware; their judgments here are down to preconceived website category prejudices. Coupled with past Spyware infections and news media articles, this has probably changed survey respondent's internet browsing habits, making them more cautious in terms of what they look at. This 'hit-and-miss' approach to computer security knowledge is probably down to a lack of access to simple and good computer security education, jointly associated to possible apathy to understand what is already there.

Somehow home PC users must be taught, or re-taught how to reduce their security risks via updating their operating system with security patches, as well as how to correctly configure, patch and use their security software i.e. Anti-Spyware software. Conversely, legislation must be looked at accurately to remove the potential 'grey area' of Spyware usage. As it can be argued that Spyware can be in some part positive to home PC users and at other times negative. This Spyware segmentation must be created to remove possible legal prosecution of possible positive 'grey area' Spyware software.

REFERENCES

AOL/NCSA (2005). AOL/National Cyber Security Alliance (NCSA) online safety study. National Cyber Security Alliance., pp.1-11.

Awad, N. F. and Fitzgerald, K. (2005). The deceptive behaviors that offend us most about Spyware. Communications of the ACM, 48, (8) pp.55-60.

Freeman, L. A. and Urbaczewski, A. (2005). Why do people hate Spyware? Communications of the ACM 48, (8) pp.50-53.

Moshchuk, A., Bragin, T., Gribble, S. D. and Levy, M. H. (2006). A crawler-based study of Spyware on the web. Proceedings of the 13th Annual Network and Distributed System Security Symposium (NDSS 2006). February 2006. pp.17.

Qing, H. and Tamara, D. (2005). Is Spyware an internet nuisance or public menace? Communications of the ACM, 48, (8) pp.61-66.

Sariou, S., Gribble, S. D. and Levy, H. M. (2004). Measurement and analysis of Spyware in a university environment. ACM/USENIX Symposium on Networked Systems Design and Implementation. San Francisco, CA.

Warkentin, M., Luo, X. and Templeton, G. F. (2005). A framework for Spyware assessment. Communications of the ACM, 48, (8) pp.79-84.

Webroot Software Inc (2005). State of Spyware Q3 2005. Webroot Software Inc., pp.1-91.

Zhang, X. (2005). What do consumers really know about spyware? Communications of the ACM 48, (8) pp.44-48.

COPYRIGHT