Accessing Spyware Awareness and Defences amongst Security Administrators

M.Koliarou and S.M.Furnell

Centre for Information Security and Network Research,
University of Plymouth, Plymouth, United Kingdom
e-mail: info@cscan.org

Abstract

Spyware threats have become very dangerous in recent years and the extent of the problem is increasing every day. Spyware works sneakily and underground, without giving signs of its presence in order to remain unnoticed, and trying to fool users in order to be installed in their systems. Therefore, to fight the spyware problem, it is very important to ensure awareness amongst end users. Many researchers found that the end users hardly understand security issues. So within organizations, there is a key role for Security Administrators. These have the responsibility for the company's security, therefore is very important to know about all of threats in high extent. This paper shows the results that gathered from a number of interviews amongst companies' Security Administrators about their awareness of spyware threats and their actions regard to security, their opinions, and their thoughts. This research found that the majority know much about spywares and much more about security defences. However, there are some respondents that did not know some features of spyware behvaiour and underestimate the threat and avoid some important actions.

Keywords

Awareness of Spyware, Security Administrators, anti-spyware adoption

1 Introduction

The extent and the power of Information Technology are increasing every day. New attractive facilities are developed on the Internet and encourage people to go online for more and more of their activities. This online world also risks many dangerous consequences. One of the security risks is the spyware threat, which can cause serious problems to both home users and to companies. The level of threat caused by spyware is sometimes underestimated because the activities often appear as harmless (Hunter, 2004). Some spyware can used for a good and helpful purpose such as to remember the user's preferences in a commercial web site in order to give an effective experience when the user visits again the site. However, it can also steal personal information such as email addresses, credit card numbers and passwords and finally they may slow down the Internet connections, and may lead to system instability and crashes (Cordes, 2005).

In the recent years, the extent of the spyware problem has increased significantly. Consequently, IDC analysts predicted that the market for antispyware products would grow from $12 million in 2003 to $305 million by 2008 (Furnell S, 2005). It seems that the extent of spyware problem is in high levels.

Spyware threats should not be underestimated and end users should take all the appropriate countermeasures in order to prevent the threat. The required safeguards are anti-spyware products together with end user awareness in order to avoid some risky activities. In order to be taken the appropriate measures by the end users, they have to be aware of those threats and how important is to protect themselves. Because users can install spyware when clicking pop ups, downloading pirate music or videos, and shareware, their knowledge about the threat plays a key role to the extent of the problem. After that, they should also be aware of how the security products are used. According to Microsoft Chief Privacy Strategist Peter Cullen, people are concerned about their online security/privacy, but have little understanding of the threats they face (LeClaire, 2009).

2 Findings of interviewing Security Administrators

This research involved face-to-face interviewing of 20 Security Administrators and IT Managers working for companies in Limassol, Cyprus. Due to the aim of the research the interviews questions addressed two subjects. The first was the participants' awareness about spyware threats and the second was their awareness about related protection. Therefore, the interviews began with questions that refer to general knowledge about spyware threats and then continued with questions that refer to anti-spyware products.

Through the interviews it was intended to establish the Security Administrators' thoughts about spyware threats, whether they find them dangerous and what they think about them when compared with other threats. Therefore, from these thoughts we can estimate the extent of their awareness about spyware threats. Also, when taking into account their actions regarding spyware protection, we can estimate their awareness about spyware defences. To assess and decice if the respondents were aware of something or not, we analyzed whether they said something relative, similar or if they did not mention it at all even though they could have. The results include some possible reasons that maybe explain the participants' answers, but without suggesting that this is a categorical or absolute interpretation.

2.1 Awareness of spyware characteristics

The interview firstly sought to establish what respondents thought about the extent of the spyware danger. Many felt that spyware threats are very dangerous, as answered by half of the respondents. The fact that the danger of a spyware depends on the type of the spyware involved was only mentioned by 6 respondents. They notified that there are types of spyware that are harmless but there are others that may cause a lot of damage and therefore being very dangerous. Furthermore, 4 out of 20 think that spyware threats are not very dangerous. That means that a minority of respondents potentially underestimated the danger of spyware programs.

The second key point was what respondents know of spyware sources, and the ways that it can intrude into the system and the network. The infection by opening a prohibited email was referred to by 10 respondents. Meanwhile, infection by visiting a malicious website was mentioned by 15 respondents. Further routes, such as downloading files, clicking pop-ups, and insertion of infected media, were all referred to by a minority of respondents (with each identified by 5 persons or fewer).

2.2 Awareness of Spywares' impact

An important possible effect of spyware programs is that they may steal confidential, personal or other kind of information by spying upon the user's actions, and send them to third parties. Surprisingly this effect, which is the main purpose of spyware, was only mentioned by 15 respondents. The lack of awareness of possible spyware effects connected also with the lack of awareness of the spyware risk level. If respondents do not be aware what spyware is able to do, they will also underestimate the spyware's risk level for a company.

Half of the respondents mentioned that another effect of spyware threats is that they slow down the operations of the computer or the network. This answer was referred from more respondents than other more serious spyware effects, such as destroying data, causing system instability and crashes, or damaging the whole system etc. The lack of speed of the operations is arguably a *symptom* that shows the spyware infection rather that a serious spyware effect. The aim of a spyware is not to slow down the operations but it has more serious damages. That shows that the 50% of the respondents, which answered that as an effect. Thus the respondents may be giving undue attention to visible consequences and disruptions rather than to the real and dangerous consequences that a spyware could have.

2.3 Awareness of Spywares' risk level

The participants were asked in a question of the interview to identify the level of risk for spyware compared to other threats. To this question all respondents directly indicated how they rate the spyware's risk level and some of them they also compared the spyware with other threats such as viruses, Trojan horses, and spamming. In the first case, 13 respondents considered that spyware has a high risk level, while the other 7 considered it medium risk. Some respondents compared the spyware threat with other threats that they face in the organization. They said if spyware is more or less dangerous than other threats such as viruses, Trojan horses, and spamming. Some respondents compared spywares with viruses, with 5 respondents considering that the latter are more dangerous. In contrast, 3 respondents think that spywares are more dangerous than viruses. Compared with spamming, 2 respondents said that spam emails are more dangerous, perhaps overlooking that spyware can be used by spammers in order to steal email addresses or other information that help them to send spam emails. Therefore, spyware's power plays very important role to the spamming threat.

2.4 Security Administrators confidence

Due to their education or training and most important due to their experience, it was expected that respondents would feel confident about their skills on spyware threats, because they are not just an ordinary end user. However, none of them suggested that they were ‘very confident’, and only a quarter indicated that they felt confident and knew a lot about spyware,. The most common response, from 9 respondents, was to suggest that they felt quite confident or fair. Unfortunately, 5 respondents did not feel confident about their skills and knowledge about spyware threats. These respondents may need to search more about that threat in order to be more aware about it, since their position rather obliges them to have knowledge and skills about all of threats in order to be able to protect the company from them.

2.5 Promoting spyware awareness to the end users

It is recognised that end-user awareness about spyware threat plays an important role in the prevention of spyware since the threats coming from the Internet. So, probably the company’s protection is depends also to the behaviour and the awareness of its employees. Therefore, it was expected to find that Security Administrators do whatever it takes in order to promote awareness to the employees. The majority of the respondents (70%) said that they inform their employees about the threats and they also guide them to their actions in order to avoid any infection. However, 2 out respondents claimed to wait until they spotted a threat in the company and then alert users or the owner of the infected computer to be more careful. Unfortunately, even worse, 4 respondents claimed not to inform the users at all about the spyware threats and how they can protect themselves and the company agsinst them.

2.6 Use of anti-spyware technologies

Most Security Administrators prefer to use one product for all the computers, but 8 indicated that they used several products to different computers because they think that having several sets of computers protected by different anti-spyware products is better protection.

One of the questions that refer to spyware detection and the way of protection that each IT Manager choose, was how often they scan the computers with the anti-virus or anti-spyware products. Most of respondents prefer to schedule the scanning to be done automatically rather than to do it manually. Everyone schedules the frequency of the automatic scan and setting the system. Nine respondents schedule a daily scan, while 2 do it twice a week, 7 schedule the scanning once a week, and finally 2 only perform a scan once a month.

When asked about the effectiveness of the anti-spyware products that they use, all respondents said that they found them effective, but none product can be 100% effective because threats every day are updated. Security Administrators do not expect the anti- spyware product to detect all of the threats, so they do not expect more from that they already get about that product, therefore they feel satisfied with what they can get.

The respondents were also asked if they trusted the protection from the anti-spyware products. Here, while 6 indicated that they trusted them, a further 8 indicated that they trusted them but not completely, as the products are able to find only the known threats and not the new ones, and new threats are emerging every day. Also, they trust them more for the prevention and less for the cleaning. They need to search for other tools in order to clean some spyware. By contrast, 6 respondents said that they did not trust them, but had no choice but to use them.

2.7 Security Administrators Actions for cleaning Spyware infections

All respondents said that firstly they wait for their products to remove the threats automatically. If their products cannot remove the threat, Security Administrators have to do some actions to clean the system from the spywares. In those cases, a quarter of the respondents are trying to find and remove the threat manually from the registries. Meanwhile 8 respondents preferred to research on the Internet to find how the spyware can be removed. They search for patches for their existing products or other tools that they can use in order to remove the threat manually. For 6 respondents, the manually cleaning of spyware is time consuming. Therefore, they prefer to re-format the infected computer. Some indicated an order of preference to their approaches, trying first to remove spyware manually, but then formatting the computer if it still remained.

2.8 Following News and Developments about Spyware Technology

Another important action that Security Administrators can do to improve their awareness about spyware threats is to follow related news and developments. Since the participants are Security Administrators and are responsible for the company's security, it was expected that they are following news about security threat included spywares. Nine respondents answered that they follow news and do the appropriate steps in order to be fully informed by following news frequently. A further 3 suggested that they followed news and developments but not to a satisfactory level. The remaining respondents admitted that they did not try to remain informed about spyware threats and technology.

3 Conclusions

The research as a whole was very informative due to the fact that the participants were Security Administrators or IT Managers for medium or large organizations (i.e. real-world professionals facing practical security issues). In general, respondents are aware of the spyware threat as a dangerous Internet risk and having also in their minds the other threats they trying for the better protection of the company. The majority of the respondents are aware that the spyware threats are spying the users' actions and can steal very important information. They are also aware of the risk level for the company. While, the majority showed that they are aware of the problem and feel quite confident to deal with it, it seems that there are some that still underestimate the threat. This finding is significant given that respondents are Security Administrators or IT Managers.

The findings in relation to the Security Administrators' actions about protection provide rather more relief, since that they are aware of what they have to do. Each company has its own plan about protection according to the company's needs and to the number of its computers, servers and employees. Differently from the protection policy and the network topology of each company, the point that this research referred was the use of anti-spyware programs. The research found that every respondent used anti-spyware products, even though many do not trust them completely or find them 100% effective.

Overall, this research with the methodology of interviews finds interesting results that show the extent of Security Administrators' awareness of spyware threats and their protection actions. Indeed, while other researcher have found that end users may not know much about spyware, it is fortunate that Security Administrators generally appear to have a high extent of awareness of the threat and can protect their company's safety acccordingly.

4 References

Cordes, C. S, "Monsters in the closet: Spyware awareness and prevention", *Educause Quarterly*, 2005, Number 2, pages 53-56, online on http://net.educause.edu/ir/library/pdf/EQM0526.pdf

Furnell, S, "Internet threats to end-users: Hunting easy prey", *Network Security*, Vol. 2005, Issue 7, July 2005, Pages 5-9

Hunter, P, "New threats this year", *Computer Fraud and Security*, Vol. 2004, Issue 11, Nov 2004, Pages 12-13

LeClaire, J, "Data Privacy Day Seeks to Raise Awareness", CIO TODAY, January 28, 2009, http://www.cio-today.com/story.xhtml?story-id=64370