1-1-2010

Ignorant Experts: Computer and Network Security Support From Internet Service Providers

Patryk Szewczyk
Edith Cowan University

Craig Valli
Edith Cowan University

10.1109/NSS.2010.42

2010 Fourth International Conference on Network and System Security

Ignorant Experts:

Computer and Network Security Support from Internet Service Providers

Patryk Szewczyk
secau – Security Research Centre
School of Computer and Security Science
Edith Cowan University
Perth, AUSTRALIA
p.szewczyk@ecu.edu.au

Professor Craig Valli
secau – Security Research Centre
School of Computer and Security Science
Edith Cowan University
Perth, AUSTRALIA
c.valli@ecu.edu.au

Abstract - The paper examines the advice and support provided by seven major Internet Service Providers in Australia through late 2009 and early 2010 in relation to computer and network security. Previous research has indicated that many end-users will attempt to utilise the support provided by Internet Service Providers as a simple and effective method by which to obtain key information in regards to computer security. This paper demonstrates that in many cases the individuals working at the help desk are either reluctant to provide IT security support or have insufficient skill to provide the correct information.

Keywords-component; SoHo; computer security; network security; survey; internet service provider

I. INTRODUCTION

The increasing popularity of broadband connectivity worldwide is permitting individuals to share and access a high-speed Internet connection easily. Numerous Internet Service Providers (ISPs) are shipping ADSL routers preconfigured with the client's username and password thus eliminating the difficulty faced by novice computer users in accessing the Internet. However, these pre-configured ADSL routers do not include pre-enabled security mechanisms such as firewall rule sets, wireless encryption, disablement of the Dynamic Host Configuration Protocol (DHCP), or access control lists. Whilst omitting the security mechanisms may reduce the time required to setup and use the wireless network, it does expose the end-user to many related threats.

Recent studies have identified two main concerns facing the end-user. Firstly, much of the literature encompassed with ADSL routers does not meet any publication standard [1]. As a result this makes using product manuals tedious as the process of locating information, navigating through sections, often interpreting low resolution graphical images and finding definitions for computer jargon creates a significant burden on the end-user. Secondly, end-users are in many instances faced with the dilemma of seeking IT support from third parties to appropriately configure and secure their networking devices [2]. In an Australian study [2] conducted in 2009, individuals claimed that they relied upon computer retail outlets and Internet Service Providers (ISP) as a means by which to seek support and guidance for issues with their Internet connectivity. In addition, many end-users perceived those working within ISP's as a group of experts.

Whilst an ADSL router may appear as a simple device, it does permit an end-user to configure the device in a manner which may either make the entire network vulnerable or relatively safe from numerous types of attacks. New threats to ADSL routers are emerging on a continuous basis [3, 4] and as a result it is important that end-users apply appropriate security mechanisms to their device. However, applying secure configuration to the router does require a certain level of skill and knowledge above that of the average end user. As a result many end-users who lack this knowledge of IT and security may find the process very challenging and discouraging.

An emerging and re-occurring threat to poorly secured ADSL routers is malware. In the first quarter of 2009 new forms of malware had been detected which targeted ADSL routers. An ADSL Router based malware - Psyb0t was hijacking consumer grade networking devices with the intention of creating a sophisticated and un-detectable botnet [3]. The malware acted on human ignorance. Consumers may not always update the device's firmware and change the password from the default. As a result the malware was distributed with a pre-populated list of 6,000 username and 13,000 password combinations which was able to infiltrate many consumer ADSL routers. As a result these devices may have not only attacked other networking devices, but may also have significantly degraded an end-users online experience.

Specifically there are two initial security procedures that can be applied to ensure that an ADSL router is protected from threats such as malware. Firstly, the end-user should change the username and password to something other than the default [5]. The password should not be a dictionary word and one that is sufficiently strong - normally greater than fifteen characters. Secondly, the latest applicable firmware update should be applied to the device which in many cases due to sales or shipping delays can be several revisions newer than the installed version [6]. Whilst the first security technique is simple, the second security

978-0-7695-4159-4/10 $26.00 © 2010 IEEE
DOI 10.1109/NSS.2010.42

technique is reasonably technical and may stop many end-users from applying this effective safeguard.

ISP's do allocate resources to creating a knowledge base of computer and network security related support. Unfortunately, a vast amount of this information may not be updated or built upon for a considerable amount of time [7]. In the instance of the Westnet knowledge base, numerous supportive pages are as much as three years out of date. In addition specific advice relates to products or techniques which are no longer viable for many modern operating systems or security products. As a result, an end-user may find this information difficult to utilize, further encouraging them to contact the ISP via telephone for direct advice.

II. Analysis of ISP Support

Studying the perceptions and attitudes of computers users has its merits in that researchers may identify the problems that lead individuals into becoming victims of Internet crime. This activity in turn permits countermeasures and educational resources to be developed to ameliorate any identified issues. Previous research has uncovered that many end-users feel more comfortable communicating directly with another individual whom they perceive to be an expert in the field of security [8]. In addition, research has identified that end-users actively communicate with an ISP as a first point of contact as they perceive these groups to have a broad spectrum of skill sets to address their computer related issues.

To date there have been no studies which have analysed and identified the merits of an end-user contacting an ISP to seek advice. One of the advantages of utilising an ISP for support is the availability of twenty-four hour and seven day access to live support. In contrast many traditional computer retail outlets may only be accessible for a fragment of this time – during business hours. In addition, unlike a computer retail outlet, there is no need for the end-user to leave their home or office which may be convenient for an end-user wanting to address their computer issue after hours [9]. Contacting an ISP has its virtues in that the end-user can be directly in front of their computer or ADSL router should step-by-step guidance be required.

This paper investigates the security advice and guidance provided by a number of popular Internet Service Providers during a three month period spanning between 2009 and 2010. A total of seven ISPs within Australia were contacted during this time which included;

- iinet
- Westnet
- Bigpond
- TPG
- iPrimus
- Dodo
- Optus

The researcher made contact two times with each ISP via telephone. Each call was initiated at a different time and day to increase the probability of communicating with an alternative technical support person. The same questions were used during each of the communications. The researcher who is knowledgeable in the area used a form of deception in that they undertook the entire conversation as a naive and ill-skilled IT end-user. The technical support individual was unaware as to whom they were directly communicating with or the specific skill set of the caller. In many instances ISP's state that the conversation will be recorded for training or educational purposes. The researcher specifically requested that this be disabled prior to the conversation. A series of three questions were directed at each of the technical support individuals. Each response was documented in terms of the actual support provided, and the willingness and supportive nature of the technical support. The three questions used in this study included:

- I would like to secure my ADSL router. What security measures or advice can you provide?
- I plan on using a wireless network at home. Do I need to do anything to secure my wireless network?
- Are there any additional security measures that you believe I could apply for my computer, ADSL router or network?

To further prepare for this research, a workstation and ADSL router were setup with no security enabled. In the event that the technical support person was willing to provide step-by-step instructions, this would allow the researcher to provide reasonable responses on the current system state if questions were raised. The ADSL router which was used was a D-Link G604t, which had wireless enabled and all security settings disabled. The workstation encompassed Microsoft Windows Vista Business, with automatic updates disabled and no security applications were installed.

It was not the aim of this study to criticise or expose inadequate technical support within ISPs. Hence, to ensure anonymity, each ISP will hereafter be referred to as ISP#-A or ISP#-B etc. The number represents the ISP and the letter represents the respondent with whom the researcher communicated.

III. Results

The results indicate that the majority of the ISPs used in the study are reluctant to support naive and ill-skilled end-

users when it comes to security. In addition, the support provided by the various ISPs demonstrates that many of the individuals working on the help desk have little knowledge in computer and network security, and as a result provided incorrect or inconsistent advice.

From the seven ISP's selected to participate in this study, only one company refused to provide any support. At any point in which a question concerning security was raised the ISP in question would immediately respond with various comments specifically detailing that they were not authorised to provide computer or network security assistance. Whilst this may be perceived as detrimental to helping the end-users with security, it does prevent the ISP from providing inadequate or flawed support. The remaining six ISP's provided varying degrees of support as demonstrated by the analysis below.

A. Question 1 – ADSL router security

The first question that was raised to each ISP was regarding general security advice for the ADSL router (D-Link G604t). ISP1 when contacted both times employed technical support individuals that were not only happy and willing to provide guidance, but were also knowledgeable in the area. In this instance, the help desk support employee provided advice in terms of guiding the researcher through; disabling the wireless radio, enabling Network Address Translation (NAT), ensuring firewall rule sets were enabled, and finally a step-by-step process of applying a full firmware update. Whilst the employees provided information in their own unique method the overall advice was sound and applicable.

Alternatively, the remaining five ISP's provided advice which may have not only confused an end-user, but also deterred them from applying any security. One of the prevailing outcomes was the complete lack of awareness of actually being able to apply 'security' to an ADSL router. The various responses provided by the ISP's support included;

ISP5-A - "...ADSL routers do not have security settings..."

ISP6-A - "...the Internet has plenty of information which may be accessed freely..."

The responses demonstrate an overall deficient approach in providing adequate support on these matters. The comment provided by ISP6-A appears that the ISP is attempting to shift the *"supportive role"* to information located online. This behaviour contradicts previous research in that Szewczyk and Furnell [2] identified that many end-users dislike utilising the Internet to locate helpful resources as they are difficult to find and more importantly untrustworthy. ISP5-A response reveals a complete lack of knowledge regarding ADSL routers. Whilst the devices do in fact encompass features to secure the device, the simple portrayal of the device as not being a securable entity may in fact reasonably deter the end-user from locating or applying any security measures. In this instance, it would have been more appropriate for the employee to simply state, that they were unaware, or unable to provide guidance in this area.

In a number of instances the technical support individual attempted to manipulate their way out of answering the question. In particular ISP6-B raised the comment that the device's security is dependent on the state of the computers to which it is connected. When this comment was questioned, ISP6-B simply stated that the Internet is accessed via the computers and that an ADSL router is simply a converter of analogue and digital signals. As a result the researcher was being convinced that ADSL routers can simply not be secured by any manner.

B. Question 2 – Wireless security

When each ISP was contacted on their recommendations to ensure that the wireless network is secured, many failed to provide adequate support. In two instances the researcher was referred to the manual that was supplied with the ADSL router. When the researcher questioned the resource and stated that they could not understand the information provided, the technical support individual reiterated that everything that is needed to secure the wireless network is supplied in the manual and that this should be referred to. Alternatively the researcher was instructed to communicate with the manufacturer of the device for further assistance. These responses clearly do not address the reported issues and does not assist an end-user in securing their device. In a recent study [1] it was identified that ADSL router literature supplied with many of the products does not meet any specific publication standard. In addition, it was discovered that in many instances the information supplied is flawed to the point whereby the process of applying security would either deter or confuse the end-user.

When ISP1 was contacted, as per the first question the same high quality of support was re-iterated for providing guidance for securing a wireless network. ISP1 provided clear instructions to the researcher into how to implement Wi-Fi Protected Access – Pre-shared Key (WPA-PSK) encryption. WPA-PSK is a robust and secure data encryption method and hence an ideal solution that each ISP should be recommending. ISP1 employees also took it upon themselves to question the necessity for using wireless in the first place. In this case the potential threats and security flaws of using this convenient yet problematic

communication medium were explained ensuring that the researcher was clearly aware of the potential pitfalls.

Alternative comments by technical support staff at alternative ISP's were not as supportive. Four ISP's stated that providing advice or recommendations for securing a wireless network is not part of their job description. One technical support individual in particular was honest and stated that they would have liked to provide assistance but did not have the expertise to provide sufficient and correct information. Additional comments made by staff employed within ISPs are;

ISP1-A - "...you need to use WEP, find this in your manual and follow the instructions..."

ISP6-B - "...you do not need to use any security for a home wireless network..."

ISP1-A stated that the researcher should use Wired Equivalent Privacy (WEP) and that the instructions would be clearly located in the product manual. Whilst WEP does provide a basic level security, it is not the paramount solution available for wireless networking. The second response is more interesting, in that the ISP6-B attempted to convince the researcher that there was no need for security if using a wireless network at home. After the researcher questioned this in more detail, ISP6-B explained that it is very uncommon for a home network to be targeted. To further compliment this poor advice it was further stated that any security mechanism that is applied would not only slow down the wireless network, but may also make utilising the network much more complex. The technical support individual further added that incorporating a significantly more complex method of operation would not be suitable for a simple user. As with the previous question, five respondents referred the researcher to seek advice from shops and retailers specialising in computer and networking products.

C. Question 3 – Extra security

The last question that the researcher asked referred to any specific advice or recommendations for securing the computer itself. In most instances the technical support individual stated that they provide support with networking and ISP related issues and not end-user computer security. However, the technical support individual in most cases was still able to provide guidance and suggestions. One of the more significant and disturbing comments was that the computer would be safe as it sits behind an ADSL router. As a result there is no need to specifically configure or install any additional security mechanisms on the computer as the ADSL router will provide adequate security. However, it was this same individual who also stated that ADSL routers do not actually have any security configuration settings that can be manipulated or applied.

In relation to providing computer security support, the respondents were slightly more educated. Firstly, ISP3-A, ISP4-B and ISP5-B recommended that an anti-virus and firewall product be installed. Secondly, ISP3 and ISP4 recommended that the Windows update feature be enabled and configured so that updates are downloaded and installed automatically. However, only ISP4 was able to provide the researcher, a step-by-step walkthrough as to how to ensure that Windows update was enabled. In addition ISP4 also provided guidance on how to download a free version of an anti-virus product. The support provided by ISP4 ended there and no additional support was provided for installing or setting up the product. The remaining phone calls resulted in technical support individuals which were quite unenthusiastic with comments including;

ISP1-A - "...you should consult Harvey Norman or a computer shop for help..."

ISP3-B - "...search for computer security on Google..."

ISP6-B"...by default Windows is a secure software product, it already incorporates a firewall and virus removal products, so you should not waste money on third party products..."

This study has identified that there is a continuous promotion by the ISP to encourage end-users towards seeking advice and purchasing goods from various IT related retail outlets. The comment by ISP3-B suggests that simply undertaking a search for *computer* security in Google will provide plenty of adequate resources. As of March 10th 2010, the exact same search in Google resulted in very few relevant and more importantly simplistic information resources that an end-user could potentially utilise. This demonstrates that an end-user may in fact struggle to locate appropriate information and in-turn may eventually relinquish their quest to apply appropriate security to their computer.

The comment by ISP6-B suggests that Windows is secure by default. However, flaws and vulnerabilities are continually published in both print and online resources. These vulnerabilities depict the new threats which have been discovered towards Microsoft Windows operating systems [10, 11]. Furthermore, these comments may diminish the probability that end-users will explore literature to apply the appropriate security safeguards to counter current and future threats.

IV. CONCLUSION

The aim of this study was to investigate the advice and recommendations provided by a number of popular ISP's within Australia. Previous research identified that many end-users attempt to seek advice from ISPs as they believe these *experts* are both trustworthy and knowledgeable in the realm of computer and network security. This study has shown that in most instances, an end-user will not be provided with factual and appropriate information for applying sufficient security. Whilst there isn't a single answer to addressing computer and network security issues, there do exist ideal solutions which could be applied. In particular numerous technical support staff stated that Microsoft Windows by default is sufficiently secure. However, this is not the ideal security strategy for an ill-skilled end-user.

Each response appears to be subjective to those who were involved in the communication at the time of the investigation. This does not necessarily reflect that all technical support individuals would address each of the issues in the same manner. One of the issues to consider within this research is that end-users may perceive ISP employees as experts and knowledgeable. However, further investigation may reveal that the role of a technical support individual may in fact be linked to a young adolescent employee who has just begun their career in IT. Hence, without adequate training and knowledge, the quality of support that can be provided will be limited and possibly flawed. End-users interpret ISP's as a convenient and highly accessible, twenty-four hour, seven day business. As a result it could be perceived as beneficial, for ISPs to train their employees to be able to provide at a minimum, an elementary level of computer and network security support to its customers.

This study has identified the quality of the support provided by a number of ISPs within Australia. If an ISP continues to provide misleading or inappropriate information they should either make it clear upon answering the call that they will not provide security related support, or state this on their website. Until each ISP makes this apparent to its customers, end-users will continue to have misleading perceptions which will result in poor and ineffective security approaches applied. This study in-conjunction with previous research has identified that computer retail outlets are perceived as also encompassing the expert characteristic. Hence future work will examine the advice and recommendations provided by computer retail outlets in Australia – hopefully uncovering whom end-users may in fact trust in this deceitful online world.

V. REFERENCES

1. Szewczyk, P. and C. Valli, *Insecurity by Obscurity: A Review of SoHo Router Literature from a Network Security Perspective.* Journal of Digital Forensics, Security and Law, 2009. **4**(3): p. 5-16.
2. Szewczyk, P. and S. Furnell. *Assessing the online security awareness of Australian Internet users*. in *8th Annual Security Conference*. 2009. Las Vegas, NV.
3. Baume, T. *Netcomm NB5 Botnet – PSYB0T 2.5L*. 2009 [cited 2009 September 10]; Available from: http://users.adam.com.au/bogaurd/PSYB0T.pdf.
4. McMillan, R. *Chuck Norris botnet karate-chops routers hard*. 2010 [cited 2010 23 February]; Available from: http://www.pcworld.idg.com.au/article/336938/chuck_norris_botnet_karate-chops_routers_hard/.
5. Symantec. *Linux.Psybot—Is Your Router Secure?* 2009 [cited 2010 March 2]; Available from: http://www.symantec.com/connect/blogs/linuxpsybot-your-router-secure.
6. Hunt, S.R. *New worm can infect home modem/routers*. 2009 [cited 2009 December 11]; Available from: http://apcmag.com/Content.aspx?id=3687.
7. Wilson, M. *Security*. 2009 [cited 2010 March 11]; Available from: http://myhelp.westnet.com.au/display/home/Security.
8. Furnell, S.M., P. Bryant, and A.D. Phippen, *Assessing the security perceptions of personal Internet users.* Computers & Security, 2007. **26**(5): p. 410-417.
9. Poole, E.S., et al. *Computer help at home: methods and motivations for informal technical support*. in *Conference on Human Factors in Computing Systems* 2009. Boston, MA, USA
10. Howard, M., *Improving Software Security by Eliminating the CWE Top 25 Vulnerabilities.* IEEE Security and Privacy, 2009. **7**(3): p. 68-71.
11. Lawton, G., *On the Trail of the Conficker Worm.* Computer, 2009. **42**(6): p. 19-22.