Edith Cowan University
Research Online

Australian Information Security Management Conference

Security Research Institute Conferences

2007

How safe is Azeroth, or, are MMORPGs a security risk?

An Hilven
Edith Cowan University

Andrew Woodward
Edith Cowan University

Originally published in the Proceedings of 5th Australian Information Security Management Conference, Edith Cowan University, Perth Western Australia, December 4th 2007
This Conference Proceeding is posted at Research Online.
http://ro.ecu.edu.au/ism/34

How safe is Azeroth, or, are MMORPGs a security risk?

An Hilven
Andrew Woodward
School of Computer and Information Science
Edith Cowan University
ahilven@student.ecu.edu.au
a.woodward@ecu.edu.au

Abstract

Massive Multiplayer Online Role Playing Games (MMORPGs) are at a basic level a networked application. Blizzard's World of Warcraft is currently the largest example of such a type of application, with over nine million subscribers at last count. Whilst the idea of researching a game for network security may sound trivial, nine million potential backdoors into home and business computers is not. The ports used by the game, as well as authentication methods and client update programs were examined using packet analysis software. No obvious vulnerabilities were discovered as a result of this analysis. In addition to this analysis, an examination of the literature in terms of other types of attack that are present was also performed. These include such common attacks as SPAM, malware and trojans. The conclusion is that while no specific network vulnerability appears to exist in the games launcher or updater, there are still a number of other attack vectors that need to be considered and protected against.

Keywords

MMORPGs, network security, spam, malware, social engineering

INTRODUCTION

"If the World of Warcraft were a nation, it would be the 90th (out of 236) most populated country on earth according to the CIA's World Factbook."

This statement was made by Videogamesblogger (2007) after Blizzard announce on July 24 of this year that World of Warcraft ("WoW"), a Massive Multiplayer Online Role Playing Game or "MMORPG", had reached the milestone of nine million subscribers. Only a few months earlier, in January, the company already announced 8 million players worldwide. All these nine million subscribers play the game through the Internet, and need to be able to do so without attackers being able to maliciously interfere with their game play. These malicious activities can range from infecting PCs with Trojans or viruses, to harassing players within the game world through scams and SPAM.

Do these types of interference with game play exist? Absolutely. Are World of Warcraft players aware of possible security threats? Sometimes... For example, in March of this year, CNet News (Terdiman, 2007) reported that WoW player Dag Friedman discovered that his account was banned due to "account sharing". In this particular example, Mr. Friedman's password was stolen. He acknowledged that in his it was a security issue, or the lack of, given that password protection is a basic tenet (Terdiman, 2007).

Some may argue as to the need for a paper such as this to be written, but there are several reasons. Firstly, there is the fact that over nine million people use this particular application on their computers. Secondly, whilst the average age of players is given to be approximately 28 years (Yee 2005), you only need to examine the voice and text chat in game to determine that there are a number of younger players on the many servers that exist. It is likely that these younger people are not likely to be as familiar with network security concepts and methods as are older players, and they may therefore be more at risk. Thirdly, with so many people using this application, if there is vulnerability present, it gives potential exploiters over nine million potential targets.

This paper will look into which ports are used, the purpose they are used for, and whether or not they are all really needed to play the game. Next, it will analyse if an attacker can intercept any personal information of a player. After all, malware that collects user information already exists, and is able to gather World of Warcraft login credentials. But is it also possible to simply sniff the network for these credentials, or are they sent to the server in an encrypted manner? And once inside Azeroth, the virtual world? There have been several news articles already about spam, scams and the like within the game (BBC News 2007; Messmer 2007). Furthermore, malware already exists that is known to transfer in-game 'money' to other accounts without the

player's knowledge. Possibly of even more concern is that reputable publishers have produced books such as *Hacking World of Warcraft* (Gilbert and Whitehead 2007).

NETWORK SECURITY

The first section of this topic, network connectivity, will list the recommendations made by Blizzard to World of Warcraft players with regards to their security devices. More specifically, it will explain which ports should be opened or forwarded on player's routers and firewalls, and why this is necessary. The second section, traffic analysis, will examine these ports as explained by Blizzard to determine whether or not it is really necessary to open each one listed. The third section, server security, will have a brief look at the servers used by World of Warcraft and their security.

Network connectivity

According to Blizzard's European online FAQ (Blizzard, n.d.), gamers playing World of Warcraft from behind a router need to configure their router to allow or forward inbound traffic from 3724/TCP and 6112/TCP. Players can also benefit from having ports 6881/TCP through 6999/TCP open or forwarded as well. Blizzard's explanation for allowing port 3724/TCP is that it is used to play World of Warcraft itself, i.e. all network communications while playing. This port is also used by the Blizzard Downloader, as well as port 6112/TCP. For ports 6881/TCP through 6999/TCP no explanation is given. However, as this is the default range used by BitTorrent traffic, analysis was conducted to verify if the BitTorrent protocol is indeed used for communications with the World of Warcraft network.

To remind players of possible security implications, Blizzard does note that forwarding ports may reduce network security, and advises to contact someone knowledgeable in the field of networking for more information. The online FAQ (Blizzard, n.d.) gives the same explanation and advice to users playing from behind a hardware or software firewall.

Traffic analysis

In order to perform individual analysis of each step from starting the World of Warcraft executable through to the process of logging in to the game, separate captures were created. Note that the full packet dumps are not included within this paper, only those relevant to the argument.

Blizzard launcher

When clicking the World of Warcraft executable, the first thing visible in a non-modified base setup is the Blizzard Launcher. This launcher displays game related news and community news, while also showing the version number of the client in the window title bar.

Running Wireshark at the time of opening the Blizzard Launcher reveals that only port 80 (HTTP) communications are made to 80-239-178-129.customer.teliacarrier.com. A WHOIS lookup confirms that the destination is indeed on the Blizzard network (Figure 1).

```
inetnum:      80.239.178.0 - 80.239.179.255
netname:      FR-BLIZZARD
descr:        Blizzard Entertainment
descr:        Entertainment Software Developer
country:      fr
admin-c:      IM4024-RIPE
tech-c:       AL5843-RIPE
status:       ASSIGNED PA
notify:       *******@telia.net
mnt-by:       TELIANET-LIR
changed:      *******@telia.net 20040428
source:       RIPE
```

Figure 1: WHOIS lookup for the Blizzard launcher program.

The first request made to this server after establishing the connection is a simple HTTP get request as shown below (Figure 2). The file downloaded here, Launcher.txt, appears to contain the version number of the Launcher available on the server. It is suspected that this is used to compare with the local Launcher version to verify if an update is needed.

```
0000   47 45 54 20 2f 75 70 64 61 74 65 2f 4c 61 75 6e  GET /update/Laun
0010   63 68 65 72 2e 74 78 74 20 48 54 54 50 2f 31 2e  cher.txt HTTP/1.
0020   31 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 42  1..User-Agent: B
0030   6c 69 7a 7a 61 72 64 20 4c 61 75 6e 63 68 65 72  lizzard Launcher
0040   0d 0a 48 6f 73 74 3a 20 38 30 2e 32 33 39 2e 31  ..Host: 80.239.1
0050   37 38 2e 31 32 39 0d 0a 0d 0a                    78.129....
```

Figure 2: http get request made by the launcher after startup

After confirmation that the HTTP request was successful, the server reveals that it is a Fedora server running Apache 2.0.50 (Figure 3). Of course this is only true if Blizzard did not change the response in order to hide the server's true identity.

```
0000   53 65 72 76 65 72 3a 20 41 70 61 63 68 65 2f 32  Server: Apache/2
0010   2e 30 2e 35 30 20 28 46 65 64 6f 72 61 29 0d 0a  .0.50 (Fedora)..
```

Figure 3: World of Warcraft runs on Linux?

The next event in the sequence is the downloading of the World of Warcraft and community news. Communication to receive this information is done to *launcher.wow-europe.com/*en and *eu.scan.worldofwarcraft.com*. The first can also be opened with a regular browser, and will contain the exact same information as visible in the Blizzard launcher. All this traffic again occurs via port 80 (HTTP).

Login screen

Once the "Play" button is clicked in the Blizzard Launcher, the actual Login screen is loaded. This starts with a DNS request for *status.wow-europe.com/en/alert* (Figure 4). This page will be downloaded to publish alerts in the login screen. These alerts usually contain information such as unexpected maintenance, available updates, or announcement of problems on certain servers. This communication is also done via port 80 (HTTP).

```
0000   47 45 54 20 2f 65 6e 2f 61 6c 65 72 74 20 48 54  GET /en/alert HT
0010   54 50 2f 31 2e 31 0d 0a 55 73 65 72 2d 41 67 65  TP/1.1..User-Age
0020   6e 74 3a 20 42 6c 69 7a 7a 61 72 64 20 57 65 62  nt: Blizzard Web
0030   20 43 6c 69 65 6e 74 0d 0a 48 6f 73 74 3a 20 73   Client..Host: s
0040   74 61 74 75 73 2e 77 6f 77 2d 65 75 72 6f 70 65  tatus.wow-europe
0050   2e 63 6f 6d 0d 0a 43 61 63 68 65 2d 43 6f 6e 74  .com..Cache-Cont
0060   72 6f 6c 3a 20 6e 6f 2d 63 61 63 68 65 0d 0a 0d  rol: no-cache...
0070   0a                                               .
```

Figure 4: DNS request for the WoW status site to inform users of realm status and other news

Everything else on the login screen is loaded from local data on the player's hard disk, so that it does not need to be downloaded over and over again. This other information consists of for example the Terms of Service, basic configuration settings, account settings, etc.

Authentication

The next step a World of Warcraft player takes to start the game would be to enter his user credentials in the login screen and click the 'Login' button.

The first thing that now happens is a new DNS request, this time to eu.logon.worldofwarcraft.com. At the moment of this research, a DNS reply was received for 16 login servers, being 80.239.180.110-117 and 80.239.178.109-116. After this moment, communication starts with one of the login servers, and traffic is no longer sent via port 80 (HTTP) but only via port 3724 (named 'blizwow' by Iana.org). In the packet dump the username is clearly readable as it is sent to the login server (Figure 5).

```
0000   00 03 25 00 57 6f 57 00 02 00 01 24 18 36 38 78  ..%.WoW....$.68x
0010   00 6e 69 57 00 42 47 6e 65 3c 00 00 00 c0 a8 01  .niW.BGne<......
0020   02 07 41 48 49 4c 56 45 4e                       ..AHILVEN
```

Figure 5: Username being sent in clear text during the login phase, but password not visible

The password, however, does not seem to be sent in an unencrypted manner, as it is nowhere to be found in the clear in the packet dump.

Blizzard Downloader

Once logged in successfully, the World of Warcraft client will automatically do a version check to ensure it is up to date with the latest patches and updates for the game.

If in fact an update is needed, the client will automatically restart and the Blizzard Downloader will be launched (Figure 6). Initial communication with the Downloaded occurs via port 80 (HTTP) to to /update/Downloader.ini, in this case on 80.239.178.131. This is immediately followed by communication on port 3724 (blizwow) to *80-239-178-125.customer.teliacarrier.com*, which as indicated earlier is part of the Blizzard network. This server's response contains an announcement for *eu.tracker.worldofwarcraft.com*.

```
0170   31 2e 37 0d 0a 48 6f 73 74 3a 20 65 75 2e 74 72  1.7..Host: eu.tr
0180   61 63 6b 65 72 2e 77 6f 72 6c 64 6f 66 77 61 72  acker.worldofwar
0190   63 72 61 66 74 2e 63 6f 6d 0d 0a 41 63 63 65 70  craft.com..Accep
01a0   74 3a 20 2a 2f 2a 0d 0a 0d 0a                    t: */*....
```

Figure 6: Initial tracker announcement for the downloader

Next, the download of the patch starts. This appears to be done through two methods. One is via simple HTTP transfers, the other are transfers via port 3724 (Figure 7). Now it is visible that port 3724 is used for BitTorrent-like traffic, indicating that a first guess earlier about the use of the BitTorrent protocol was correct.

```
0000   13 42 69 74 54 6f 72 72 65 6e 74 20 70 72 6f 74  .BitTorrent prot
0010   6f 63 6f 6c 00 00 00 00 00 00 00 00 bd 20 4d c6  ocol......... M.
0020   0f 81 30 0c 71 37 13 ec 69 e6 e8 11 62 d0 d1 4d  ..0.q7..i...b..M
0030   42 4c 5a 00 07 71 bc a3 86 32 3c fb be ea 04 18  BLZ..q...2<.....
0040   18 82 52 12                                      ..R.
```

Figure 7: Start of the patch download using a BitTorrent protocol

Various connections are now established with IP addresses all over Europe, most of which are dynamic addresses from ISPs. This indicates that BitTorrent connections are made to download updates via other World of Warcraft players connected to the Blizzard Downloader at the same moment.

A quick look for traffic on ports 6881/TCP through 6999/TCP reveals that these ports are indeed also used by the Blizzard Downloader to connect to World of Warcraft gamers using the BitTorrent protocol on the default BitTorrent ports. Earlier research by Messer (n.d.) and Avery (2007) found similar results for World of Warcraft servers in the Americas, seemingly confirming the findings in this section.

BitTorrent security

Even though BitTorrent often has a negative connotation, it appears that Blizzard succeeded in implementing this protocol in a secure way for use with the World of Warcraft client. Searching for vulnerabilities, bugs or exploits present in the Blizzard implementation of the BitTorrent protocol have not revealed any known information with reference to potential security issues.

A test was done to connect to a host while it was downloading World of Warcraft updates through port 3724/TCP. Output of the netstat –an command confirms the host is listening on this port, as it should (Figure 8).

```
C:\Documents and Settings\WowHost>netstat -an
Active Connections
  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:3724           0.0.0.0:0              LISTENING
  TCP    192.168.1.2:139        0.0.0.0:0              LISTENING
  TCP    192.168.1.2:2701       217.43.127.137:3724    LAST_ACK
  TCP    192.168.1.2:2761       82.181.116.45:3724     ESTABLISHED
  TCP    192.168.1.2:2765       81.164.244.207:3724    ESTABLISHED
  TCP    192.168.1.2:2900       83.216.57.17:3724      ESTABLISHED
  TCP    192.168.1.2:2910       85.164.24.29:3724      ESTABLISHED
```

```
TCP    192.168.1.2:2913       85.29.235.207:3724     ESTABLISHED
TCP    192.168.1.2:2920       85.227.168.94:3724     ESTABLISHED
TCP    192.168.1.2:2929       81.225.228.136:3724    ESTABLISHED
TCP    192.168.1.2:2938       213.112.205.175:3724   ESTABLISHED
```

Figure 8: A list of the active connections during the BitTorrent update process

A telnet connection to the downloading host on port 3724 is successful, yet the information received only confirms this port is used by the BitTorrent protocol. No possible way was found to interact further with this host.

```
C:\Documents and Settings\TestHost> telnet 192.168.1.2 3724
BitTorrent protocol¢ Mãü0
                                q7ýiµÞbðÐMBLZq╝úå2<¹¥Û♦éR↕☺B☻@☺►    ☺Ç@►☻!$☻♦@☻♦@♦@☺►
☻☻☻☺@Ç►D☻ ►@ ►└►ÇÇÇ♦♦☺
```

Figure 9: Succesful Telnet connection made to the downloading host on port 3724

A connection attempt was made to the same host by using the official BitTorrent client with a connection on port 3724. This connection was not successful either.

Server security

Very little information is known about the security of Blizzard's World of Warcraft network and servers. As probably could have been expected, it was also quite impossible to receive any information from Blizzard concerning this topic. The only information received was to simply read through the official website and forums, and no further information would be provided.

Although a quick Nmap and/or Nessus scan would likely result in some interesting facts, this type of reconnaissance was not performed due to legal issues that might rise.

Exploits

It appears that the World of Warcraft servers are either quite good protected and up to date with patching, or these servers are not a much wanted target of attack. This can be concluded from the fact that only one successful exploit was found that was in fact able to shut down the servers. This was the result of a bug in the virtual world, not even by a bug on the servers hosting it. Although Blizzard was able to fix the bug within a few hours, it was not disclosed what exactly caused the bug (Modine, 2007). It is also unknown whether or not Blizzard has sufficient security and logging in place to discover who abused this bug, and if corrective actions were taken against these users' accounts.

This concludes the topic of general network security as relevant to World of Warcraft players, or network/security administrators of organizations that allow this activity on their network. The next section will explain which threats exist against the security of World of Warcraft game accounts, and how to diminish them.

ACCOUNT SECURITY

This topic will have a look at the security of World of Warcraft game accounts. More specifically, it will delve into the existing threats against these accounts. The first section, threats, will explain why there is a threat against account security. This will be partially based on information from Symantec's Internet Security Threat Report, but will also look at measures taken by eBay to protect both buyers and sellers of virtual goods. In the second section, malware, known malware that can affect World of Warcraft players in general will be discussed. The most seen techniques and pieces of malware will be discussed, including malware created by attackers to obtain account information. Last, although unrelated to stealing login credentials, this section will also look at potential spyware from Blizzard itself. The third section, client security measures, will list security measures that can be taken by players. This part will be touched only briefly, as these measures are not much different from those that any PC user in general should take.

Threats

Research by Symantec, discussed in their Internet Security Threat Report of March 2007 (Symantec, 2007), reveals that a stolen World of Warcraft account is more valuable than a United States based credit card with verification value (Table 1). Therefore it is quite understandable that nowadays some attackers start focusing on stealing WoW account information instead of credit cards. Due to the fact that World of Warcraft accounts and

virtual goods can be stolen, the legal complexities of auctioning virtual goods made eBay decide in January of this year to ban this kind of auctions. As explained by eBay, its policy states that the seller must be the owner of the underlying intellectual property, or be authorized by the owner to do so. Because ownership in online games is hard to prove, eBay's intention is to remove the possibility to sell what might be goods in fact owned by someone else (Zonk, 2007).

Table 1: Advertised prices of items traded on underground economy servers (Symantec, 2007)

United States-based credit card with card verification value	$1–$6
United Kingdom-based credit card with card verification value	$2–$12
An identity (including US bank account, credit card, date of birth, and government issued identification number)	$14–$18
List of 29,000 emails	$5
Online banking account with a $9,900 balance	$300
Yahoo Mail cookie exploit—advertised to facilitate full access when successful	$3
Valid Yahoo and Hotmail email cookies	$3
Compromised computer	$6–$20
Phishing Web site hosting—per site	$3–5
Verified PayPal account with balance (balance varies)	$50–$500
Unverified PayPal account with balance (balance varies)	$10–$50
Skype account	$12
World of Warcraft account—one month duration	$10

Because the original source of malware is often very hard to determine, let alone trace which goods or credentials were stolen, the situation as explained by eBay appears to point in the direction of malware that can be used to gather these goods and account credentials. Therefore, it is indeed nearly impossible to verify whether or not the seller is in fact the real owner of the auctioned goods.

Malware

Viruses, worms, Trojans

As seen earlier, adversaries can make more money by stealing World of Warcraft accounts than they can by stealing credit cards. Hence, several forms of malware already exist, most of which have only one sole purpose: stealing login credentials for World of Warcraft accounts.

One technique used is exploiting a known vulnerability in animated cursor handling under Windows operating systems (CVE-2007-0038). By targeting this flaw, login data can be captured and sent back to the creator of the exploit.

Other exploits that can be used for the same purposes are against known vulnerabilities in either the Microsoft Data Access Components (MDAC) or in Vector Markup Language. Malicious websites containing one of these exploits will transfer and install a Trojan baptised "Infostealer.Lingling" by Symantec (Wang, 2007). This Trojan will search for the Chinese World of Warcraft window, and collect information such as the server being played on, username, password, operating system information and the local IP address. Once collected, this information will be submitted to the creators of the Trojan. The Trojan "Infostealer.Wowcraft" serves the same purpose, in that it is used for harvesting passwords (Park, 2005), yet no detailed information is available about its way of working.

Mass-mailing worms can also come into play when it comes to stealing credentials. One example is the worm W32.Wowlook@mm (O'Connor, 2007). It will change registry entries for Outlook Express, allowing the user to open attachments that are usually denied by default. This will enable the user to download the Trojan, which will in turn steal World of Warcraft account information, and continue its rampage by spreading itself through email addresses it gathered from Outlook Express and Windows Address Book.

Rootkits

Although no rootkits are currently known to exist with the purpose of interfering with World of Warcraft clients, there is one rootkit that is not very much liked by Blizzard, namely the Sony BMG software. The cloaking abilities of this rootkit can be manipulated in such a way that cheating mechanisms used by the player go

unnoticed by Blizzard's game monitors (Crawford, Malikov, Miller, 2006). These monitors were in fact created to prevent cheating, and are better known as "The Warden", which will be discussed in the next section.

Spyware

Not only can attackers use spyware to collect information, Blizzard itself has integrated a small form of spyware in the World of Warcraft. However, opinions differ as to whether or not this piece of software, "The Warden", falls under the category of spyware. Greg Hoglund of rootkit.com, and author of "Exploiting Online Games: Cheating Massively Distributed Systems" (2007), disassembled The Warden and in turn wrote "The Governor", which's sole purpose is to monitor what The Warden monitors (Hoglund, 2005). He concluded that this application reads memory for the processes running at the moment it runs, being every 15 seconds. The reason The Warden does this is to make sure players are not running anything that would enable them to cheat (Cohen, 2005).

As it was found that The Warden checks all running processes, and does not collect any personal information, for many people it would not fit in their definition spyware. For some people, this definition would be that spyware is software installed without the users consent (Hoglund, n.d.). For others, this definition is based on the fact whether or not the software sends personal data somewhere for marketing purposes (Hoglund, n.d.). The Warden does not fit any of these two definitions because a) it does not collect and submit personal information, and b) the player allows for The Warden to be used by agreeing to the Terms of Service contract, which states the use of monitoring software (Cohen, 2005).

Technically speaking, however, The Warden should be considered as being spyware. Even though no information is sent back directly to Blizzard (instead it is compared against a list of hashes (Hoglund, n.d.)), the Terms of Service state that "some" information will be sent to Blizzard (Messer, n.d.), without further elaborating on which information this exactly concerns. Therefore, even though it is unknown which information is sent to Blizzard, World of Warcraft activity should be banned on corporate or other networks where classified of proprietary information is present.

Client security measures

Choice of security packages

Seen the technique available to steal account information, using strong login credentials simply is not enough. Making use a good anti-virus program and some common sense (TenTonHammer, 2007) is already a very good start, and neither of these is hard to use. Several freeware anti-virus programs do an excellent job, and common sense will prevent one from downloading potentially malicious third-party plug-ins and add-ons. Moreover, even if these third-party packages are safe, their use is not allowed in the EULA and can result in Blizzard banning the account.

Because a lot of malware makes use of known vulnerabilities to get access to the player's PC, it is of utmost importance that when playing World of Warcraft on a Windows system, the system has the latest patches available.

Blizzard from their side also makes work of client security. The Blizzard Launcher, which can be used to start the World of Warcraft session, will scan a player's PC and alert the player if maliciously looking activity such as key logging occurs (Terdiman, 2007). Unfortunately, the Blizzard Launcher is a piece of software that can be easily disabled by the player. It is suspected that the majority of players do this, in order to get to the login screen faster and skip a step before being able to play. No information, such as which anti-virus vendor or signatures are used for detection, could be found about this scan for malware.

Choice of operating system

Although not supported by Blizzard, an extra layer of defence can be added by running World of Warcraft under Wine in a Linux environment. Players with adequate Linux knowledge can set up a basic environment only including Wine and the WoW client itself. (WoWWiki, n.d.)

Even though a lousily set up Linux system can be just as insecure as an unpatched Windows system, the trick is that Linux systems will allow further lockdown of processes and services, adding more security to the system. Furthermore, Linux is usually a lesser target of attack than Windows.

CONCLUSION

This paper has demonstrated that whilst the launcher, login and update aspects of this MMORPG appear to be adequately secured, other security risks present in other web networked technologies, such as email and internet banking, are still present. These include spam, social engineering and malware, which are threats to all internet

and web users, and not just gamers. It is important that users understand that whilst they are playing a game, what they are using is an application which has the potential to be exploited the same as any other network application. Future research could explore the psychological aspect of game playing, and whether they are less likely to take seriously the security risks that are present.

"My suggestion? Monitor the hell out of your computer for items running that you don't know, change your password on a regular basis, and don't get too attached to the items you've collected, because tomorrow they might not be there."

That's what Michael Fahey (2007) wrote when he discovered his World of Warcraft account was hacked into, and everything sellable had been sold. When a client running World of Warcraft is not properly protected, this would indeed be the best advice and conclusion to end with. However, wouldn't it be a lot smarter to secure the client to avoid credentials and virtual goods to be stolen or altered instead of not getting too attached to them? After all, an attacker simply does not have the right to do this, so why let him?

REFERENCES

Avery, J. (2007). Decoding the World … of Warcraft. TippingPoint DVLabs. Retrieved on September 24, 2007, from http://dvlabs.tippingpoint.com/blog/2007/06/28/decoding-the-world-of-warcraft

BBC News (2007). Cursor hackers target WoW players. Retrieved on September 24, 2007, from http://news.bbc.co.uk/2/hi/technology/6526851.stm

Blizzard (n.d.). Configuring Your Firewall for use with World of Warcraft and the Blizzard Downloader. Retrieved on September 25, 2007, from http://faq.wow-europe.com/en/article.php?id=291

Blizzard (n.d.). Configuring Your Router for use with World of Warcraft and the Blizzard Downloader. Retrieved on September 25, 2007, from http://faq.wow-europe.com/en/article.php?id=292

Blizzard (2007). World of Warcraft surpasses 8 million subscribers worldwide. Retrieved on September 26, 2007, http://www.blizzard.com/press/070111.shtml

Blizzard (2007). World of Warcraft surpasses 9 million subscribers worldwide. Retrieved on September 26, 2007, from http://www.blizzard.com/press/070724.shtml

Cohen, P. (2005). WoW security issue – spyware. Retrieved on September 27, 2007, from http://www.macworld.com/forums/ubbthreads/showflat.php?Cat=&Board=UBB22&Number=362366&page=0&view=collapsed&sb=5&o=&fpart=1

Crawford, B., Malikov, O., Miller, M. (2006). Rootkits: A hidden issue in security. Retrieved on September 27, 2007, from http://www.knowbd.com/piedmont/mba605/sp061reports/rootkit.pdf

Fahey, M. (2007). WoW I feel violated. Retrieved on September 27, 2007, from http://kotaku.com/gaming/world-of-warcraft/wow-i-feel-violated-247979.php

Hoglund, G. (n.d.) Is the warden spyware. Retrieved on September 24, 2007, from https://www.rootkit.com/newsread.php?newsid=369

Hoglund, G. (2005). 4.5 million copies of EULA compliant spyware. http://www.rootkit.com/blog.php?newsid=358

Hoglund, G. (2005). Keeping Blizzard honest. Announcing the release of 'The Governor'. Retrieved on September 27, 2007, from http://www.rootkit.com/newsread_print.php?newsid=371

Hoglund, G., McGraw, G. (July 2007). Exploiting online games. Cheating massively distributed systems. Addison-Wesley

Messer, J. (n.d.). Under the Surface of Azeroth: A network baseline and security analysis of Blizzard's World of Warcraft. Retrieved on September 24, 2007, from http://www.networkuptime.com/wow/

Messmer, E. (2007). How cheaters are winning at online games like World of Warcraft. Retrieved on September 24, 2007, from http://www.networkworld.com/news/2007/072707-online-games-dirty-secrets.html

Modine, A. (2007). World of Warcraft exploit PKs servers. Retrieved on September 24, 2007, from http://www.playnoevil.com/serendipity/index.php?/archives/1542-Denial-of-Service-Attack-against-World-of-Warcraft-Hotfixed.html

O'Connor, J. (2007). W32.Wowlook@mm. Symantec. Retrieved on September 24, 2007, from http://www.symantec.com/enterprise/security_response/writeup.jsp?docid=2007-030416-3427-99&tabid=1

Park, J. (2005). Infostealer.Wowcraft. Symantec. Retrieved on September 24, 2007, from http://www.symantec.com/security_response/writeup.jsp?docid=2005-073115-1710-99

Popa, B. (2007). eBay banned World of Warcraft virtual goods auctions. Retrieved on September 25, 2007, from http://news.softpedia.com/news/eBay-Banned-World-of-Warcraft-Virtual-Goods-Auctuions-45809.shtml

Symantec (March 2007). Symantec Internet Security Threat Report. Underground economy servers. Retrieved on September 24, 2007, from http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_internet_security_threat_report_xi_03_2007.en-us.pdf, p. 32

TenTonHammer (2007). Account Security. Retrieved on September 24, 2007, from http://wow.tentonhammer.com/index.php?module=ContentExpress&func=display&ceid=531

Terdiman, D. (2006). World of Warcraft battles server problems. ZDNet. Retrieved on September 25, 2007, from http://news.zdnet.com/2100-9595-6063990.html

Terdiman, D. (2007). No end in sight to hacking of WoW accounts. Retrieved on September 24, 2007, from http://news.com.com/2100-1043_3-6174704.html

Videogamesblogger (2007). World of Warcraft hits 9 million users worldwide! Making it the 90th largest country in the world. Videogamesblogger. Retrieved on September 25, 2007, from http://www.videogamesblogger.com/2007/07/24/world-of-warcraft-hits-9-million-users-worldwide-making-it-the-90th-biggest-country-in-the-world.htm

Yee, N. (2005) The daedalus project. Retrieved September 26th 2007 from http://www.nickyee.com/daedalus/archives/pdf/3-4.pdf

Yunlong, S. (2007). Gang arrested for kidnapping online game champion. China View. Retrieved on September 27, 2007, from http://news.xinhuanet.com/english/2007-07/18/content_6392309.htm

Wang, R. (2007). Infostealer.Lingling. Symantec. Retrieved on September 24, 2007, from http://www.symantec.com/security_response/writeup.jsp?docid=2007-021415-3740-99&tabid=2

WoWWiki (n.d.). World of Warcraft on Linux. Retrieved September 27, 2007, from http://www.wowwiki.com/Linux

Zonk (2007). eBay delisting all auctions for virtual property. Slashdot. Retrieved on September 27, 2007, from http://games.slashdot.org/article.pl?sid=07/01/26/2026257

COPYRIGHT

An Hilven and Andrew Woodward ©2007. The author/s assign Edith Cowan University a non-exclusive license to use this document for personal use provided that the article is used in full and this copyright statement is reproduced. Such documents may be published on the World Wide Web, CD-ROM, in printed form, and on mirror sites on the World Wide Web. The authors also grant a non-exclusive license to ECU to publish this document in full in the Conference Proceedings. Any other usage is prohibited without the express permission of the authors.