Original Article

International Journal of Forensic Science
Volume 7 Number 1, January–June 2024

Detecting Information from MMORPGs

M Vishwanatha Bhargav[1], Don Caeiro[2]

How to cite this article:
M Vishwanatha Bhargav, Don Caeiro. Detecting Information from MMORPGs. Int Jr of Forensic Sci. 2024;7(1):25–28.

Abstract

MMORPGs are a combination of RPGs and MMOGs in which millions of players worldwide play simultaneously. MMORPG is the most popular genre of gaming among millions of people. Many crimes are taking place due to MMORPGs such as homicides, sexual offences, theft, fraud, hacking etc.

A study was conducted in order to detect information which is left by the MMORPGs in computer systems, which can also be used as corroborating evidence or real evidence connecting the suspect to the crime in cybercrime investigations.

Eight games were selected (4 browser based, 4 client based) as samples, downloaded, installed and certain number of sessions were played. The hard disk which contained the sample was analyzed using Access Data's FTK Imager for game information and chat histories. The client based games were uninstalled and analyzed as well.

We found that browser based MMORPGs did not leave any traces of chat history but it had traces of important information such as URLs and timestamps. Client based MMORPGs left a lot of vital information as well as chat history. After uninstallation, the client based MMORPGs had yielded the same data as before uninstallation, but as deleted files.

Thus, from this study we could prove that MMORPGs data can be detected and obtained from suspect hard disks and also can be used as corroborating evidence or real digital evidence which links the suspect directly to the crime in cybercrime investigations.

Context: In the field of digital forensics and cybercrime, determining the information left behind by various applications is a necessity. MMORPGs are one type of such applications that require in depth analysis as to the type of information that can be retrieved from the computer system that is being used by the games. This will further help forensic examiners to proceed in the right direction and create a protocol for analysis of such games.

Aim: To determine the information that can be retrieved from MMORPGs in a computer system.

Settings and Design: Experimental study conducted on a system with eight MMORPGs. The games were used and various activities including chatting was conducted on it and then information was searched for in the computer system.

Methods and Material: Eight games were selected (4 browser based, 4 client based) as samples, downloaded, installed and certain number of sessions were played. The hard disk which contained the sample was analyzed using Access Data's FTK Imager for game information and chat histories. The client based games were uninstalled and analyzed as well.

Statistical Analysis Used:

Results: We found that browser-based MMORPGs did not leave any traces of chat history but it had traces of important information such as URLs and time stamps.

Author's Affiliation: [1]Security Consultant, Delloite, Bangalore 560077, Karnataka, India, [2]Assistant Professor, Department of Forensic Science, Krishtu Jayanti College, Bangalore 560077, Karnataka, India.

Correspondence: Don Caeiro, Assistant Professor, Coordinator, Department of Forensic Science, Krishtu jayanti College, Bangalore 560077, Karnataka, India.

E-mail: doncaeiro@kristujayanti.com

Received on: 03.11.2023

Accepted on: 15.12.2023

Client-based MMORPGs left a lot of vital information as well as chat history. After uninstallation, the client-based MMORPGs had yielded the same data as before uninstallation, but as deleted files.

Conclusions: This study we could prove that MMORPGs data can be detected and obtained from suspect hard disks and also can be used as corroborating evidence or real digital evidence which links the suspect directly to the crime in cybercrime investigations.

Keywords: MMORPGs; Game Data; Cyber Forensics; MMORPG Game Information Forensics; MMORPG Chat History.

INTRODUCTION

The video games in which millions of gamers play simultaneously by controlling their respective avatars in a virtual world through online connectivity and also chat with other players on the game are known as Massively Multiplayer Online Role Playing Games (MMORPGs). Crimes are occurring due to spending too much time online, chatting and many other contributing factors in MMORPGs. This study aimed to determine the information that can be retrieved from MMORPGs in a computer system. The study focused on the retrieval for chat history, cache data, time stamp, frequency of web visit etc., in MMORPGs. The information obtaining from MMORPGs are used as collaborative evidence in many cases, helping the investigation agencies to find more possibilities to reach to the crimes that happening through MMORPGs.

MATERIALS AND METHODS

A total of 8 games were used to obtain game data information and chat histories in which four were client based MMORPGs and four were browser based MMORPGs. The games chosen for sample collection were Everquest 2, Star Wars: The Old Republic, Defense of the Ancients 2 (DOTA 2), AIKA Online, Battlestar Galactica Online, League of Angels, Stormfall: Age of War and Mage Realm.

1. The official websites of the games were visited.
2. New accounts were created and confirmed after providing registration details.
3. The games were logged in on web browsers, played for a certain number of sessions and logged out.
4. Chatting was done in the sessions during the game play.
5. Drive (C:) which had the web browser history and cached files was analyzed using access data Forensic Tool Kit Imager 3.2.0 (FTK).
6. On FTK Imager, the information pertaining to the browser history and cached files cannot be visualized into textual format.
7. Foxton forensic software, browser history capturer was used to capture all the browser history and cached files pertaining to web browsers in the computer system.
8. Foxton forensic software, browser history viewer was used to visualize all the captured information into textual format.
9. All the information viewed on this tool was scrutinized.
10. All observations and data findings were tabulated.

Client based MMORPGs Procedure

1. The official websites of the all the chosen MMORPGs were visited to register and download the client software of the game.
2. The account registration details were provided to the websites for sign up and the account was confirmed using the email IDs provided in the registration details.
3. The client softwares were then installed on the computer system.
4. The client softwares were executed and allowed to download and install the game data.
5. The games were logged in, played for a certain number of sessions and logged out.
6. Chatting was done in the sessions during the game play.
7. Drive (D:) which had the game data files in it was analyzed using access Data Forensic Tool Kit Imager 3.2.0. (FTK).
8. On FTK Imager, the information pertaining to the game was searched manually.
9. All the files pertaining to the game were searched for in the textual data and scrutinized.
10. All observations and data findings were tabulated.

RESULTS

Information left by Browser based MMORPGs:

Most of these games left information about which web browser was used to play the game. The time at which the website of the game was last visited was obtained. The number of times the website was visited was also recorded by the tool. All the URLs used during the game play were collected by the tool. The cached images and the "last fetched time" of the images were obtained and analysis.The cached images, its URLs and file sizes were obtained by the tool. The cached webpage URLs were also found and analyzed. One of the cached webpages of the game mage realm URL revealed the email ID and password of the user. One game, League of Angels, did not leave any traces in the computer system for analysis.

Information left by Client based MMORPGs

All these games gave information about name of the account and usernames used in the game. Launcher settings were obtained from Everquest 2 and Star Wars: The old Republic. Except AIKA Online, all the games gave information about the number of characters in the game, their names and types. Except Everquest 2, all the games gave a log contained the background processes and their time stamps. Everquest 2 and DOTA 2 gave the IP addresses of servers to which the computer connected itself during game play. Settings of the game were obtained for AIKA Online and Everquest 2. Only Everquest 2 gave the chat history of the player. All downloaded data along with time stamps were obtained for Everquest 2 and Star Wars: The Old Republic. Unique User ID and Company ID was found in Everquest 2 and DOTA 2. Except AIKA Online, the game location in the computer or the file path of game data was obtained. DOTA 2 gave the general location of the computer with the game in it as well as a log of server connections and time stamps along with IP addresses.

Specific Information and Chat History Left by MMORPGs:

Browser based games did not leave any traces of chat histories. Most of the browser based games left timestamps, URLs, cached data. Mage Realm left a cached webpage in which the URL revealed the email ID and password of the user. Everquest 2 left a log of chat history. Everquest 2 also gave a unique company ID, list of server IP addresses and usernames. Star Wars: The Old Republic left logs of background processes, data from game sessions, login and log out time stamps. Defence of the Ancients 2 (DOTA 2) left logs of background processes, server connections and time stamps, general location of the computer with the game installed. DOTA 2 also gave unique user ID and build ID. AIKA Online gave username, setting of the game and logs of background processes.

Information Left by Client Based Games after Uninstallation

Information found before and after uninstallation were found to be the same. All data were seen as deleted files in FTK Imager software which were exportable. AIKA online did not leave any normal traces of files after uninstallation. Everquest 2, DOTA 2 and Star Wars: The old Republic left residual files such as logs of downloaded data and setting of the game.

DISCUSSION

The analysis of information left by MMORPGs unveils a complex landscape of privacy and security risks. Browser based games with their tracking of web browser details, visit time and URLs, are notable threat to the privacy of the user.This can lead to a targeted attack or profiling based attack on gaming habits. The exposure of cached images and webpages by Mage Realm, underscore the significance for improved security measures. In contrast client based MMORPGs disclose detailed player information, including account names, usernames, character details etc. Raising the concern about the privacy of user and the potential for exploitation these details. The retrieval of server IP addresses, especially in games like Everquest 2 and DOTA 2, under scores the importance of securing data from breaches and potential threats by exploiting IP addresses. The presence of chat history in Everquest 2 give information regarding the user's nature and in crime related analysis the modus operandi of the attackers. In Everquest 2, DOTA 2 and Star War: The old Republic, the files was able to retrieve post uninstallation process, provides more possibility to get user information.

CONCLUSION

From the study conducted it was found out that browser based MMOPRGs did not leave any traces of chat histories during game play. It only left information of URLs, cached data, number of times the website was visited and time stamps of when the website was visited. Upon further analysis, the email ID and password of the user was also found for a particular game.

On the contrary, Client based MMORPGs left a lot of information which includes chat history during game play, server connection logs, unique IDs, game setting information, usernames, general location of the computer, IP addresses of server which the computer connected to, login and log out timestamps, activity log during gameplay and downloaded data logs.

Even after uninstallation, Client based MMORPGs yielded data as deleted files, same as before uninstallation. They also left residual files in the computer such as logs and few text files.

Thus, from this study it is proved that MMORPGs data can be detected and obtained from suspect hard disks and also can be used as corroborating evidence or digital evidence which links the suspect directly to the crime in cybercrime investigations.

REFERENCES

1. Lars Daniel, Larry Daniel, (October 2011), Digital Forensics for Legal Professionals, Elsevier Science, Syngress.
2. Leigh Achterbosch, Robyn Pierce, Gregory Simmons, (March 2008), "Massively Multiplayer Online Role-Playing Games: The Past, Present, and Future", ACM Computers in Entertainment, Vol. 5, No. 4, Article 9.
3. Ying-Chieh Chen, Patrick S. Chen, Jing-Jang Hwang, Ronggong Song, Larry Korba, George Yee, (2005) ,"An analysis of online gaming crime characteristics", Emerald Internet Research, Vol. 15 No. 3, Emerald Group Publishing Limited.
4. Madihah Mohd. Saudi, (2001), An overview of disk imaging tool in computer forensics, SANS Institute.
5. Mirko Suznjevic, Ognjen Dobrijevic, Maja Matijasevic, (2009), "Hack, Slash, and Chat: A study of players' behaviour and communication in MMORPGs", research project 036-0362027-1639, Ministry of Science, Republic of Croatia.
6. Jason Moore, Ibrahim Baggili, Andrew Marrington, Armindo Rodrigues, (2013), "Preliminary forensic analysis of the Xbox One", Digital Investigation, The International Journal of Digital Forensics & Incident Response, Vol. 10, Issue 4, Elsevier.
7. News articles of online games tracking by intelligence agencies for terrorist clues. http://www.computer world.com/article/2486632/cyberwarfare/the-nsa-tracks-world-of-warcraft-and-other-online-games-for-terrorist-clues.html.