Malwares in Online Games – A tool for hackers to invade PCs

(COMP-116)

Abstract

Online gaming has been in power for a long time now. According to a report, in 2017 there were about 2.2 billion active gamers in the world with most of them spending handsome amount of money on these imaginary scenes of entertainment. The mind-blogging speed with which this figure is increasing, it is imperative to discuss whether the games people play, and the time and money they spend on are secure enough or these are posing a serious threat on their privacy. In the recent past some serious loop holes have been figured out in the game industry making peoples' PCs vulnerable to attacks by hackers. While such foundings, which includes type of malwares loading and controlling someone's PC, affected the figure due to the game industry being questioned by people, still games are too contagious for some. An important aspect of playing on the web is that people meet with strangers not knowing the nice person they are talking to, playing with, sharing personal information with might be as nice as an intruder. It is crucial that online gaming to be made more secure and small insecure channels must be blocked so that the innocent people gaming online can thrive in a secure environment free of hackers.

Introduction

Online Gaming is not only a source of killing time but a great way to keep connected to friends. In fact, the modern online games are more like a social media platform where people share their profile, can add each other as friends, earn ranks the higher they go, chat with each other, record or send voice messages online, play together and can do a lot more. Such social inclusion in games have shifted the traffic from locally played games to online platforms. This, in addition, has also invited hackers to apply their malicious ways to hack into the server and shoot while keeping their guns on someone else's shoulder. This is a key issue and must be examined to ensure the safety of billions of people who have exposed themselves on such gaming platforms online. I would like to discuss on some critical topics in this paper such as the functionality of malwares and the ways hackers have used malwares to make their way into systems and the consequences people faced due to such attacks, extra security measures that different game platforms and game companies have used to prevent such happenings in future, the limitations of preventions and maintaining a secure atmosphere, and the measures people should take on their own to avoid such a brouhaha.

To the Community

I have myself come across people who faced such an issue and the influence of this problem is so great that the people who have been the victim of such an issue are still unsure if their PC is free of any alien working on it. People are too concerned about

their data; big companies leverage on users by providing them with storage on the web in turn for money so that the users can create a backup of their data online in case their PC gets corrupted. No matter how long passwords you keep for you account, your PC is still no way secure when it comes to gaming online. And in most of the scenarios, malware is working behind the scene. While the social media platforms keep people protected somehow where people get the choice of sharing information with only their known ones, gaming online is a new experience to meet and interact(playing) with strangers. It is possible that a stranger creates an object and upon interacting with that object one's PC is in the hands of the stranger just because the object was too suspicious to be interacted with. So, people should think the types of games they play online and how could those make their PC vulnerable to attacks by the hackers. One does not know who is sitting behind the dummy one is playing with. Awareness of such a key point is substantial to thwart off the risk involved.

The Real use of Malware in Games

In simple terms, malware is a piece of software that is used to damage a computer system. Elaborating further, these malwares can steal or alter data, override control or do some serious harm to PC. Some common forms of malware include spyware, ransomware, viruses, worms, trojan etc. There are various game providers that have ensued technical vulnerabilities and cyber-crime issues after releasing their products. These technical vulnerabilities have paved a way for hackers to build their mischievous web. While most of the malwares need some action to be taken by the victim to get activated such as a file download or clicking a popup advertisement or shooting a player etc., gaming provides the best way to achieve such initiation.

One of the popular approaches is the use of RAT (Remote Access Trojan), which is a malware, and allows control over user's PC with administrative controls. A widely played game called CS: GO (Counter Strike Global Offense) became a victim of such attack. Upon shooting an opponent, the opponent gets control of the user's PC by shifting states of player model as processed by the server followed by RAT being loaded onto victim's PC. It became much easier for hackers to implement this cunning method when an additional feature was included in the CS: GO interface i.e. players permission to create dummy players. The clever hackers programmed the dummy players to act as bridge for hackers to move to victim's computer.

There are various other ways to activate the Trojan. Most of the games involve a social network for communication between players. This communication can be in form of text message or voice message and most attackers make use of such social channels. Let's suppose your stranger friend, who plays with you every day, send you a malicious message or a weblink on your chat box and if the chat environment is not isolated from the database or is not protective against spams, you might end up opening that the

message which could be a devil's note. This is another common fashion of exposing the player nowadays. It is possible for hackers to send phishing emails or any related content to email associated with gamer's account with a set pack of instructions to follow or immediate action to be taken. These links can initiate a download of malevolent trojan on one's PC.

Trojan horse by far is a very dangerous malware which has proven lethal sometimes. There are various ways to use trojan horse. As far as games are concerned trojan is used is used in two most important ways i.e. backdoor and rootkits. While using as a backdoor, hackers can control PC as far as converting the computer into botnet for DDOS (Distributed Denial of Service Attack) attacks, rootkit is same as overriding the administrative rights of the user's over PC. Once the access to host PC is achieved, the malware can be used to steal electronic money, rob the data, start a webcam or keylogger, and even install more malwares to the system.

Another malware called 'Joao' has recently hit the game world. This malware comes with the game download files and upon launching of the game installer it can, without any disruption in the game, send system's secret information to the hacker. This information includes the OS version, name and the preferences user have on the device. Based on such information, Joao decides what types of malicious coding components needs to be downloaded. ESEST's, an online IT security company, research has suggested that Joao uses backdoor, spying and DDOS attacks for causing destruction. Joao is known to spread rapidly in the future. It mainly making use of the MMORPGs (massively-multiplayer online role-playing games) to do so.

Contemporary Hacking and overall consequence

The attacks conducted by hackers today are very different from the ones that were done a long time ago. Earlier the attacking equipment was written in Delphi making it easier for antivirus to detect, however, now hackers have invented a new strategy to release worms which can easily replicate. Although most of these malicious malwares need human intervention to get activated but the game scenario is so broad and intense that the user forgets to care about their security. And because it is a game and most of the time hackers take the advantage of your nerves, it has become a lot easier for them to take over one's data. Since these worms are masked by the rootkits, while their presence won't even be detected and thus users remain unaware of their PC being secretly monitored by a third party, the evil code can infect the device completely.

Malwares in addition to leaking user's privacy, can compromise system's computational power as well. It can cause increased CPU usage, not affording to open two heavy application at the same time even though the system is capable of doing it, lagging and crashing applications, PC getting hanged very often, automatic running of

program without user's commands and much more. The worst-case scenario is that sometimes malware can deactivate anti-virus and block firewalls to gain a better breeding ground.

Ransomware is another big issue. Ransomware is a type of malware that attackers use to decrypt some sensitive files and asks for ransom from the victim in order to decrypt those. The attackers usually use military grade encryption system such as RSA and AES. Most of the gamers care about their saved games that they have been playing for ages and in turn pay as demanded by the attacker.

Malwares could be a bad time for the game developers as well. For example, the loophole that the attacker has used to install malware on someone's computer whether it is server susceptibility or bug in the system, as far as it is due to the developer's non-robust measures, developer is usually held liable for the resulting catastrophe. The same goes for any phishing attempts or DDOS attempts. This can tarnish the reputation of the developer company and can be a harbinger of disaster both socially and financially.

Actions and Remedies

Achieving a perfect solution is not the target, which in fact might not be possible as well, however, going towards the solution is. We possibly can delve into making the finest possible measure to endure the security of one another.

Since, third-part sources have come into action, which normally provide the weakest security for users therefore, users should try not to make use of the pirate version of games and avoid downloading the games to be played online from rogue third-party sources. Failure to do so can result in a DDOS or much severe hack attempts. A perfect example is that of Joao malware that gets initiated with a suspicious '.dll' type file. It is normally named as 'mskdbe.dll'. Presence of this file is a direct indication of one's system getting effected with Joao. Therefore, a tip would be to check out for this type of file on the game downloaded directories before running the game installer.

There are a lot of internet security services and anti-malware tools available online for use. One should run multiple scans on the files to detect, if any, the presence of malwares. Also, all the software should be kept updated because whenever a vulnerability is found on a software, it should be replaced by the updated version to increase the security against the vulnerabilities.

Lavasoft is a software company that produces spyware and malware detecting software has an Ad-adware Game Edition tool which, in addition to many other anti-malware software, is a very effective tool for detecting malware. In an interview, the vice president of sales and marketing at Lavasoft Helander and Malware Lab's Andrew Brown once mentioned that Ad-aware runs uninterruptedly off the screen without

consuming much of computer's resources and this in turns makes it better for use than most other anti-malware software.

Most of the games played online are MMORPGS (Massive Multiplayer online role-playing game). People should play games that come with pre-installed anti-hack programs. Also, people should maintain some distance from the people they come to meet with in online games no matter how good they seem because after all they are strangers. Moreover, avoid sharing personal information with strangers on games. People should run PC then updated versions of anti-virus scans or anti-spywares from trusted companies on their PCs. In case they receive any email or some content on their game's social channel then they should try not to download it right away especially if is from a stranger and must take the authenticity in account before proceeding and if it is a link, one should check address behind the URL (Universal Resource Locator). In short, spamming is the technique used to spread malware and should be taken seriously.

DDOS attacks are very detrimental. According to a source, a DDOS attack lasts for about 11 hours and costs around $500,000 to fix. Latency and instantaneous load are two extremely important parts of game play and issues in such areas can back track the player from game while also taking back the money they invested. Hence, the game developers should understand that making their platforms more secure can help them save a handful amount of money because unfortunately DDOS attacks are expected to increase in number in the near future. Therefore, a need to produce a much secure game experience on web by game developing companies prevails.

Conclusion

Fighting against hacking is an endless war, and even after most extreme measures the probability of getting hacked still exist. We as humans can only take steps to minimize such incidents to the best of our abilities. This is evident by the fact that despite the efforts of tech. evangelists in the rich history of cybercrime, security bugs in systems, including the very advanced ones, are still not uncommon. Keeping aside the research point of view, an important point to quote is that apart from the security measures provided by the host, most of the security risk could be determined using acute observation. A strong sense of vigilance can act as an antidote for such breaches. In fact, when it comes to protection, in most of the cases common sense takes precedence in prevention of hacking incidents with far reaching consequences. Therefore, both an eye and preventive measures are important in determining the self-protection, and these must be implemented by gamers in the same way as they abide by the rules of the game.

Bibliography

Banks, N. (2016, February 26). *Imperva Incapsula*. Retrieved from https://www.incapsula.com/blog/online-gaming-webinar.html

DuPaul, N. (2012, October 12). *Common Malware Types: Cybersecurity 101.* Retrieved from Veracode: https://www.veracode.com/blog/2012/10/common-malware-types-cybersecurity-101

Gardoň, T. (2017, August 22). *Gamescom 2017: It's all fun and games until black hats step in.* Retrieved from We Live Securty by ESET: https://www.welivesecurity.com/2017/08/22/gamescom-2017-fun-blackhats/

Golovanov, S. (2007, September 10). *Securelist*. Retrieved from securelist.com: https://securelist.com/online-games-and-fraud-using-games-as-bait/36169/

Komando, K. (2013, July 19). *USA Today.* Retrieved from https://www.usatoday.com/story/tech/columnist/komando/2013/07/19/hacker-attack-trojan-horse-drive-by-downloads-passwords/2518053/

McDonald, E. (2017, June 20). *Newzoo Insight Articles*. Retrieved from https://newzoo.com/insights/articles/newzoo-2017-report-insights-into-the-108-9-billion-global-games-market/

Newman, S. (2016, December 19). *Corero*. Retrieved from https://www.corero.com/blog/787-ddos-for-points-how-to-beat-hackers-at-their-own-game-.html

Villanueva, J. (2017, July 20). *DOT ESPORTS*. Retrieved from dotesports.com: https://dotesports.com/counter-strike/news/frag-exploit-june-update-one-up-computer-hackers-16027

Viruses, Malware Creeping into Online Games. (2009, November 18). Retrieved from PCWorld from IDG: https://www.pcworld.com/article/182542/viruses_malware_creeping_into_online_games.html