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

By: Muhammad Sheheryar Naveed

Introduction

1. I am a (CompSci) sophomore currently enrolled in a computer security class at Tufts.
2. Gaming is a form of relaxation for many. Some popular games such as Counter Strike and Age of Empires are cross-platform multiplayer games usually played online. Being an active member of the community of online games, I have come across people discussing issues(malwares) related to online gaming that poses threat to the user ownership of their PCs!

Background

1. In reality, there's lot of data that is exchanged on the server when a person plays the game online. This includes the chat text, credit/debit card details for extra feature purchase, voice messages while on the play and much more. Most importantly your interaction with strangers. These are some of the ways hackers can use to reach out to one's PC.
2. The caveat is not playing games but playing *online* which makes one's PC vulnerable to attacks by hackers, and thus constitutes to a big cyber security risk. Awareness of such susceptibility of online games is important.

The focal point

1. Interaction with aliens one plays with is the root to all the problems. If the alien is a hacker, then it becomes very easy for the alien to infect one's computer as most virus or malwares involved requires activation and online gaming is the best way to provide such interaction without the victim's consent. Playing over nerves (i.e. rapid decision making) for many adds to the ease of hackers.

The malicious ways adopted

1. Trojan-Horse
   - Trojan-horse which is used as backdoor and rootkit. Backdoors can convert a PC into a botnet for DDOS attacks and rootkit overrides the administrative rights of the user on PC.
   - Such attempts have already been claimed by some gamers who played Counter Strike.
   - It is also possible that if the social channels such as chat boxes in games are not protective against spams then it makes the system vulnerable to Trojans. Hackers can send phishing email to users for making an immediate action which might require downloading something or in some way activate the hacking element.
2. Joao
   - Joao is a malware that comes with the game download files. A .dll type file is suspicious and specify the presence of Joao.
   - It sends the user's preferences and the OS version to attacker and then installs the malicious components accordingly.

Consequences of Attacks:

1. Techniques used for hacking today are a lot stronger than those used in the past (For e.g. worms that can replicate and are harder to detect).
2. CPU usage compromise, applications crashing and hanging and even sometimes turning off anti-virus.
3. Ransomware:
   - A form of malware that can be used to encrypt files on system and then ask the victim for money to decrypt.
   - Strong encryption used such as RSA and AES.
4. Game Developer's reputation is tarnished by users facing such attacks.

Prevention Measures

1. Avoid downloading game files from rogue or private third-party sources.
2. Use of some good anti-virus tools such as Ad-Adware, Bitdefender and Avast.
    1. One must go for authentic and licensed version of these anti-viruses and update it frequently.
    2. For malware detection, especially trojan if any malicious activity is felt, people must look for some unknown installed files or software which they don't remember installing and remove those as early as possible.
3. Users should verify any spam material before clicking or downloading the content. Checking address behind the URL is a good technique. Also, people should avoid sharing personal information with strangers no matter how good they seem. After all, strangers are strangers.
4. Keeping a vigilant eye on the community discussion for any security threat detected and take necessary action likewise as suggested by the game developer.

Conclusion

1. It is to be understood that it might not be possible to put an end to the hacking techniques, however, the goal is to minimize these attempts to the best of our abilities. Additionally, precautionary measures should be taken seriously by the online gamers.

Idea on Supporting Material:

I am probably going to stick with the third option which says a conference presentation slide deck as it appears to be the most suitable option for me. Also, I am good at making presentations.

These are some of the references that I'll use to build up my paper:

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