



# MALWARES IN ONLINE GAMES- A TOOL FOR HACKERS TO INVADE PCS

BY: MUHAMMAD SHEHERYAR NAVEED

# WHAT ARE MALWARES?

- Malware is malicious software.
- It is designed to damage computer systems,
- These can not only bring the whole machine down but also can be as harmful as stealing both data and money.
- Spywares, ransomwares etc. All are different kinds of malwares.



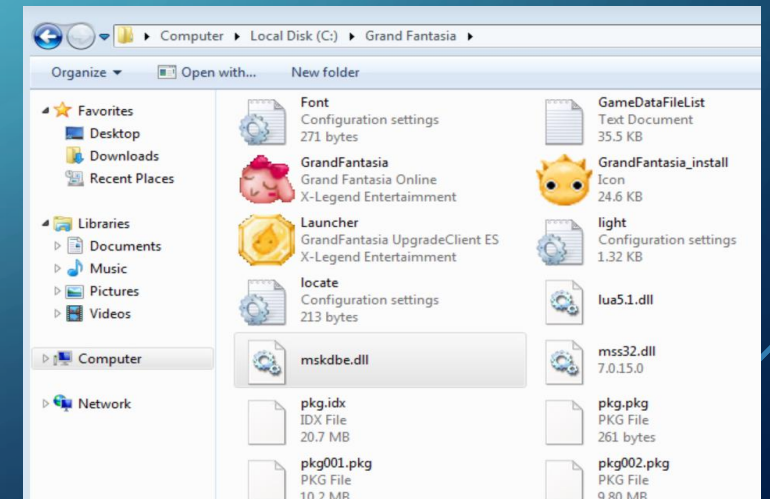
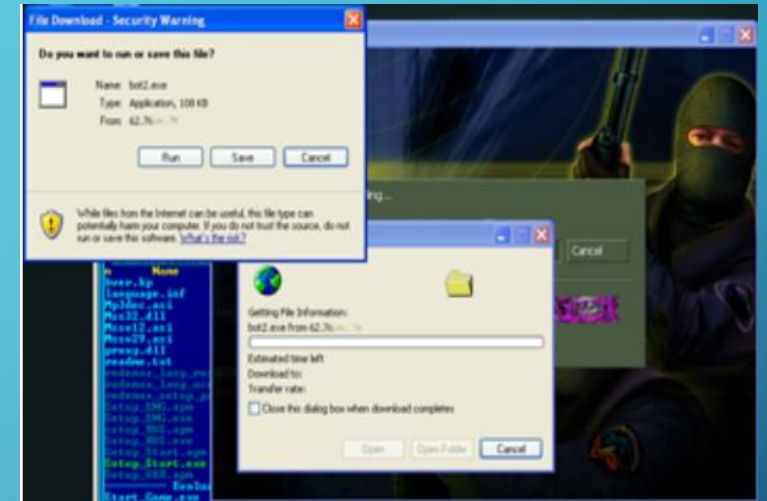
# WHY SPECIFICALLY GAMES AS A BRIDGE?

- Strangers become friends even though they have never seen each other ever before.
- Games act as a curtain for hackers. One never actually knows who is behind the dummy they are about to shoot.
- Chat environment in most of the games are breeding grounds for malicious attacks.
- Playing over the nerves(i.e. rapid decision making) add to the ease of hackers.
- Debit/Credit card details for extra feature purchase in some famous games.



# ISSUES IN THE PAST?

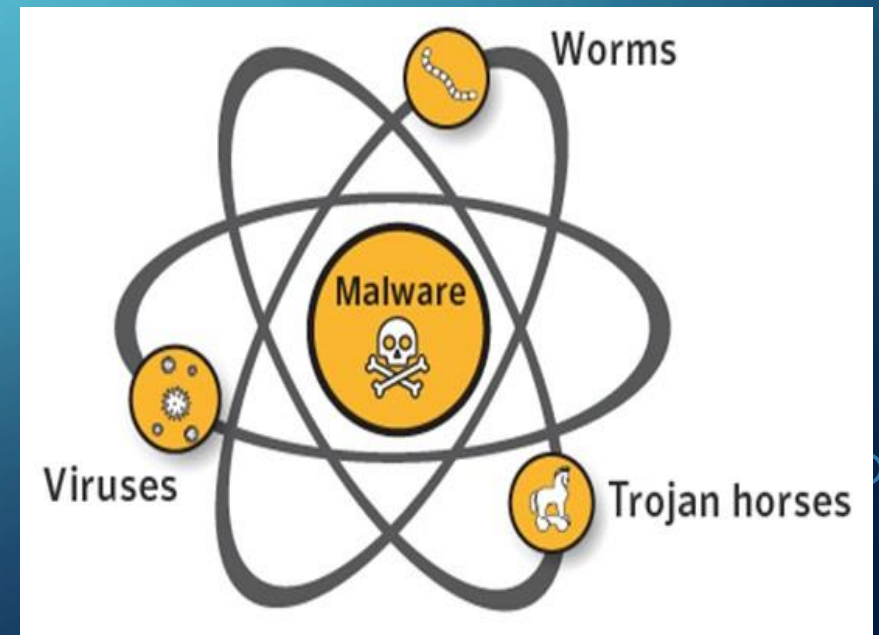
- In the recent past, some counter strike enthusiasts have faced the issue of their PCs behaving strangely which was a probable outcome of malwares. Hackers were able to embed a malicious script behind the dummy bots in online gaming which when hit gives access to shooter's PC.
- Joao has inflicted severely on Latin America Gamers.
  - Source: <https://www.bnamericas.com/en/news/ict/latin-american-gamers-worst-affected-by-joao-malware/>
- Trojan horse detected in Age of Empires 2.





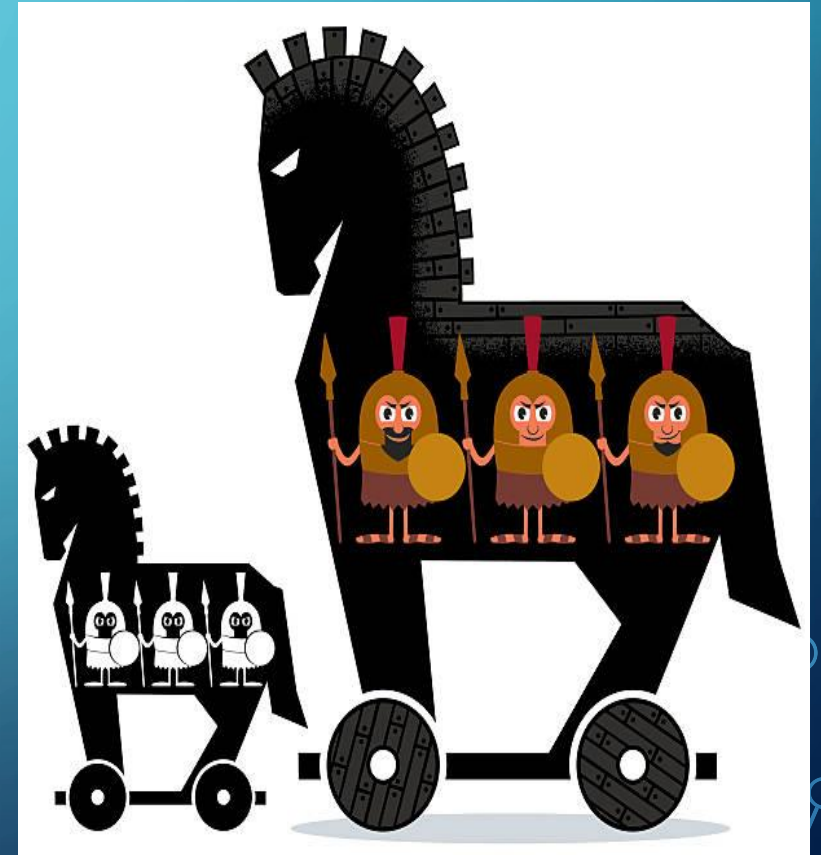
# MALICIOUS WAYS ADOPTED

- Malware needs a user action for its activation.
- Trojan-horse: The terms comes from the history of trojan war between the Greeks and the trojan.
- Joao: A virus on Microsoft Windows originating from Brazil.
- Phishing content on games that have social channels enabled.



# TROJAN HORSE

- A genuine programs that tricks the user to install it and then spreads the virus all over the computer.
- Trojan as back-door: Converting a PC into botnet for DDOS attacks.
- Trojan as rootkit: Overrides administrative rights of users on PCs.
- Chat boxes that are not protective against spams may result in phishing. This can lead to gamers downloading malicious stuff on their platforms.



# JOAO

- Joao was recently discovered as is spreading rapidly. The dirty infectious code comes with the downloaded files(.dll *type file to be more specific*).
- It sends the user's preferences and the OS version to attacker and then installs the malicious components accordingly.
- It spreads through fake MMORPGS through Aeria Games' Identity.
- There were some websites spreading the unofficial version of the Aeria Games with Joao embedded in them.

# WORMS

- Worms have provided a thriving place for attackers. Worms replicates and spreads from device to device without any human interaction.
- The difference between worms and virus is that virus needs active host program or already infected computer or active Operating System for it to run. Unless activated, the virus present inside the application remains dormant.
- Worms are stand-alone and can spread through computer network without the user knowledge. Starts to multiply itself as soon as it gets to the system.



# SOURCES OF WORMS

- Emails: Files as attachments
- Peer-to-peer file sharing networks
- Internet: A web link or a link to download FTP resource.
- Operating system vulnerabilities: An example is 'Conficker' which is a worm that exploited the network service vulnerability present in many versions of windows.
- Smart-Phones: HTML-5 based mobile applications can cause the spread of worms because one of the flaws of html-5 is that malicious code can be injected into it.

# CONSEQUENCES?

- Techniques used by hackers today are stronger than ever before.
- Increase CPU usage deteriorating the PC's life.
- Game Developers and Providers' reputation is tarnished.
- Ransomware can be an indirect result.
  - A form of malware that can be used to encrypt files on system and then ask the victim for money to decrypt.
  - Strong encryption is used such as RSA and AES.

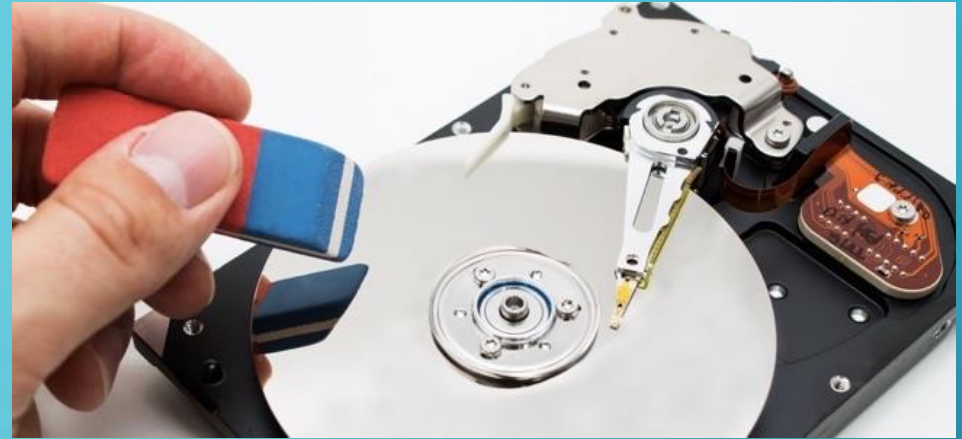
# PRECAUTIONARY MEASURES!

- Avoid downloading game files from rogue or private third-party sources.
- Use of some good anti-virus tools such as Ad-Adware, Bitdefender and Avast.
  - One must go for authentic and licensed version of these anti-viruses and update it frequently.
  - 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.
- 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.
- Keeping a vigilant eye on the community discussion for any security threat detected and take necessary action likewise as suggested by the game developer.
- Parental supervision required for children playing games on web.

# PRECAUTIONARY MEASURES!

- Firewall: To filter the incoming and outgoing traffic according to the security guidelines.
- Strong passwords: Passwords of account should be strong enough to confuse the enemy at the first place.

# WIPING THE DISK




- In a nutshell, there are a variety of types of trojan horse and each has a different functionality, thus it might be possible for these to go beyond detection even after the precautionary measures. Therefore, a crystal clear approach for wiping out virus from one's PC would be to mitigate the disk after a specific period of time(the shorter, the better).



# CONCLUSION

- **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.**

The background is a blue gradient. In the corners, there are decorative white line art elements resembling circuit boards or neural networks, with lines and small circles.

# QNA SESSION