Ethical Hacking and Countermeasures

Version 6

Module LI

Hacking and Cheating Online Games

The Electric New Paper :

CYBERGAME THEFT IN THE NEWS
Former cyber thief tells how she cleaned out one account

She tells gamer: If you love me, give me your password

SHE led a guy on, then stole from him, leaving him virtually penniless.

02 December 2007

SHE led a guy on, then stole from him, leaving him virtually penniless.

Cleaned out of his virtual wealth, that is.

Cybergame thieves were in the news recently, when one was fined $3,000.

Jenny (not her real name) claims she did it only once, a couple of years ago.

She duped an American boy she met in an online game and managed to get him to reveal his password to her.

She said she told him: 'If you love me, give me your password to prove it.'

Once she had the password to his account, she went in and plundered everything that he had painstakingly acquired after countless hours of playing the massively multiplayer online game (MMOG).

She transferred all the boy's virtual money, armour and weapons to her own MMOG account.

Jenny, barely 16, told The New Paper: 'I remember he had a few million in virtual money and I stripped him clean of his armour and gear.

'I think they were probably worth a few hundred dollars in our currency.'

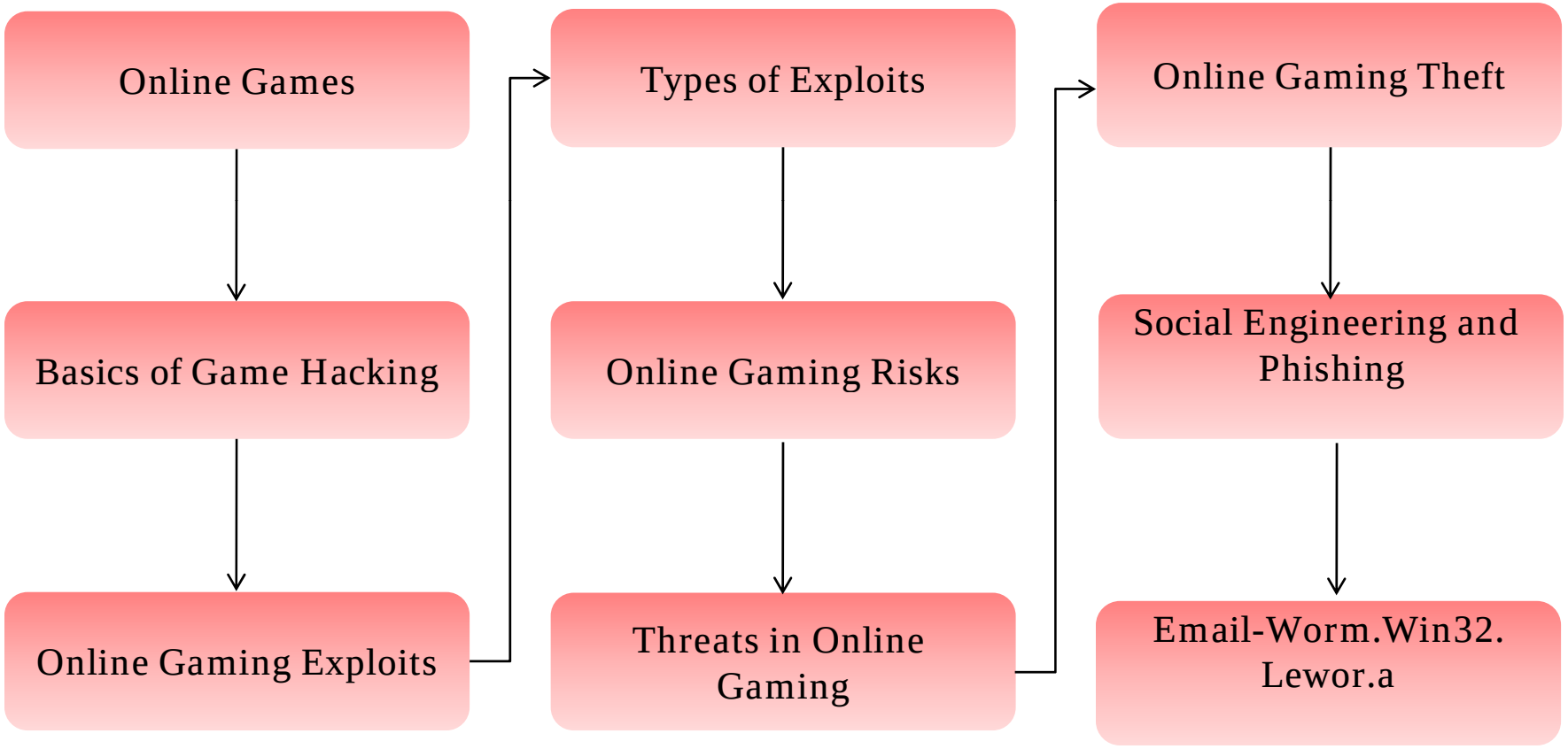
Source: *http://newpaper.asia1.com.sg/*

Module Objective

This module will familiarize you with:

- Online Games
- Basics of Game Hacking
- Online Gaming Exploits
- Types of Exploits
- Online Gaming Risks
- Threats in Online Gaming
- Online Gaming Theft
- Social Engineering and Phishing
- Email-Worm.Win32.Lewor.a

Module Flow



Online Games: Introduction

Online games are played over a computer network (the Internet)

Online games come in different forms, including simple text based games and games with high graphics

Online games associate themselves with online communities and form a social network

Basics of Game Hacking

Cheating Massively Distributed Systems, discover the various attacks and hacking techniques to target the vulnerabilities found in online games

Game hacking includes the following techniques:

- Building a bot
- Using the user interface
- Operating a proxy
- Manipulating memory
- Drawing on a debugger

Online Gaming Exploits

Online Gaming Exploit is a software bug, hack or bot that is given to the user's in a manner not intended by the developers

The consideration for this type of exploit varies between games and developers

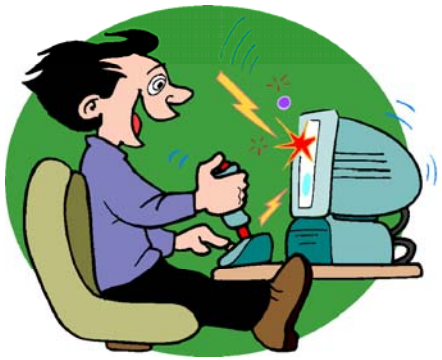
The EULA (End-User License Agreement) typically affirm what type of gameplay is not acceptable

Developers may consider First-person shooter (FPS) to be an exploit, while others may not

Types of Exploits

Wall hack:

- It is the process of changing of wall properties in first-person shooters
- Wallhack gives hidden information about the players, thus by allowing players to see objects that are present behind the wall



Aimbot:

- Aimbot is software used in online “multiplayer first-person shooter games”
- It provides guidance to the player to reach the target and gives advantage over unaided players

Types of Exploits (cont'd)

Cham hacks:

- Cham hacks are a common method of cheating in online first-person shooters
- It restores player models with brightly colored skins such as neon red/yellow and blue/green colors

Bunny hopping or Strafe-jumping:

- Bunny hopping or Strafe-jumping use both mouse and keyboard input
- The correct method and the combination depend on the game
- Most of the games follow some types of user actions
- Some FPS(First Person Shooter) Games have maps made just for this trick

Online Gaming Risks

Online gaming risks comprise the following:

- Malicious software
- Risks from viruses, Trojan horses, computer worms, and spyware
- Insecure or Compromised Gamer Servers
- Insecure Game Coding
- Risks from computer intruders
- Risks from online and real-world predators
- Risks are associated with strangers who may trick you to get personal or financial information

Online Gaming Risks (cont'd)

The intruders may want to do any of these:

- Capture your personal information
- Steal your identity
- Steal your credit card information
- Inappropriately contact children by pretending to be another child, setting up meetings, or tricking them into revealing personal information
- Cyber prostitution
- Virtual mugging
- Virtual sweatshop

Threats in Online Gaming

Gain illegal access to play the game by guessing password or acquiring it by robbery

Cheat at game play

- Collude with others to attain higher levels of play
- Use cheat program
- Buy virtual properties/skill
- Steal virtual properties/skill
- Attack on gaming software that controls play levels

Disrupt game play

- Man-in-the-middle attack on communications
- DNS (denial of service) attack
- Inside job arranges disruptions
- Release virus/worms

Threats in Online Gaming (cont'd)

Cheat while paying for game play

- Obtain copies of legitimate time card serial numbers
- Obtain card by robbery
- Dictionary attack on time card serial number
- Guess time card serial number
- Use Trojans to transmit a player's time card number
- Attack on connection time tracker software
- Inside worker at game provider arranges for free time

Steal proprietary parts of the software

- Inside worker arranges theft
- Attack on server containing desired software
- Use Trojans to transmit desired code or design documents
- Kidnap members of design team

Online Gaming Theft

- Player authorization system in most online games is based on a password system
- Online games use player authorization system to verify player authenticity
- Malicious users steal usernames and passwords to steal items, put up for auction, and sell them to get virtual money
- A cyber criminal may also demand a ransom for stolen items
- Malicious users demand money for stolen items from the users
- Malicious users target most of the online game players

Online Gaming Theft: Screenshot

70 Rogue and pally epix!

Seller of this item? Sign in for your status

1 of 2

View larger picture

Starting bid: **US $800.00** Place Bid >

Make No Payments Until 2008 Apply

End time: **Aug-27-07 15:40:06 PDT** (6 days 8 hours)

Shipping costs: Check item description and payment instructions or contact seller for details

Ships to: United States

Item location: Florence, AL, United States

History: 0 bids

You can also: Watch This Item

Get alerts via Text message, IM or Cell phone

Email to a friend

Listing and payment details: Show

Characters for sale on Ebay

A message on a gaming forum (and some appropriate Google Ads)

January 13th, 2004, 11:56 AM #1

Ginte
Junior Scribe

Join Date: Jan 2004
Posts: 5

My account is stolen:(

Hya all I play on choas server (ea)
On 2004.01.03 i lost my 2 account's and can't get them back:/ One is x1 lvl 57 fire mage Ginte and other x1 lvl 76 char V3bas
No1 can help me:(Cheater logins my characters and plays with them:/ Do U have any suggestions?:flaming:

Trojan Scanner
Top 10 Web Sites About Trojan Scanner
WebImmix.org

Trojan
Better history results & research on
Ask.com. Use Ask.com now!

Ads by Google

Quote

Methods Used to Steal Passwords

How Passwords for Online Games are Stolen

Cyber criminals steal only the user name and passwords of victim users, and not the address of server where the user is actually playing the game

Malicious users log on to the machine where the victim is actually playing

Social Engineering and Phishing

Social engineering:

- A person using social engineering try to gain the confidence of someone who is authorized to access the network in order to reveal information that compromises the network's security

Phishing:

- Cyber criminal sends phishing emails, from the server administrators, which invite player to authenticate his/ her account via a website linked in the message
- Cyber criminals enter a game or a forum on a game server and offer a bonus, or help in the game, in exchange for other players' passwords
- Malicious user achieves his/her goal (getting hold of passwords) and leaves his/ her victims with nothing

An Example of a Phishing Email

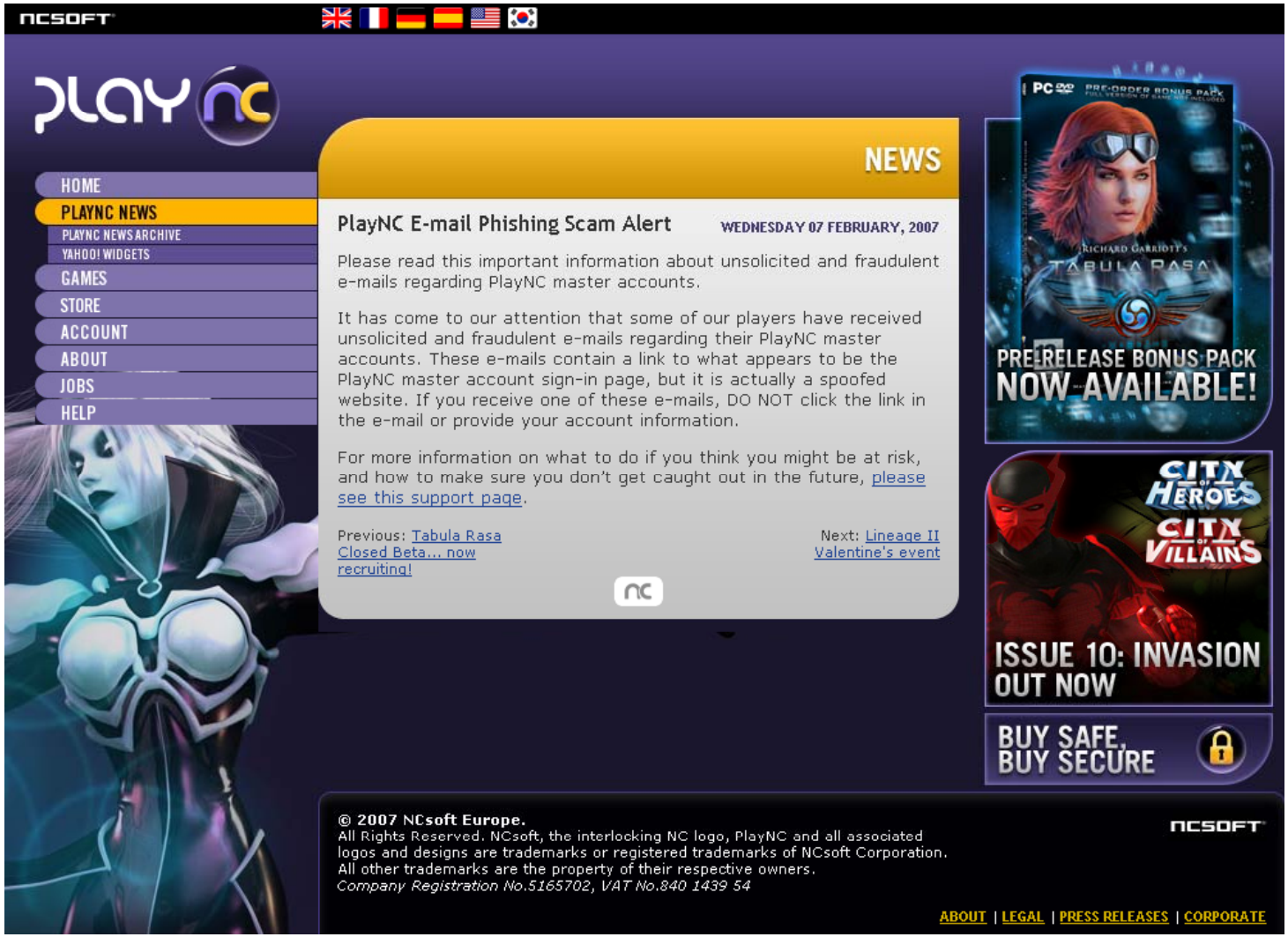
Здравствуйте.
Вы получили данное письмо так, как являетесь зарегистрированным пользователем нашего сервера (www.Lineage2.su)
В связи с тем, что количество зарегистрированных пользователей нашего сервера за последний месяц
резко возросло,мы вынуждены произвести чистку нашей базы данных. (не использующихся аккаунтов)
Для подтверждения того, что вы ещё играете на нашем сервере вам необходимо пройти аутентификацию
на этой странице:
******

Если вы не прошли аутентификацию в течении 48 часов с момента получения этого письма - ваш аккаунт будет
удалён без возможности восстановления.

С уважением администрация Lineage2.su

Hello,
You have been sent this email because you are a registered user on our server (www.Lineage2.su). Because the number of registered users of our server has increased sharply over the last month, we have to purge inactive accounts from our database. Please confirm that you still play on our server by undergoing authentification here:
If you do not authenticate your account within 48 hours of receiving this message your account will be deleted, and it will not be possible to restore it.
Yours,
The Lineage2.su administrators

News: Phishing Attack on Gamers' Accounts



Exploiting Game Server Vulnerabilities

Game Servers comes with system services, programs and databases designed to support on line games

Game server software might contain programming errors, bugs, and vulnerabilities

Attackers use these vulnerabilities to exploit the Game Server and gain access to the databases

After gaining access they execute arbitrary code and retrieve the encrypted passwords

Another way to get passwords is by clicking on forgotten passwords

Cyber criminals send mails with malicious content to the target user, then change the victim's password, and enter the game using new password

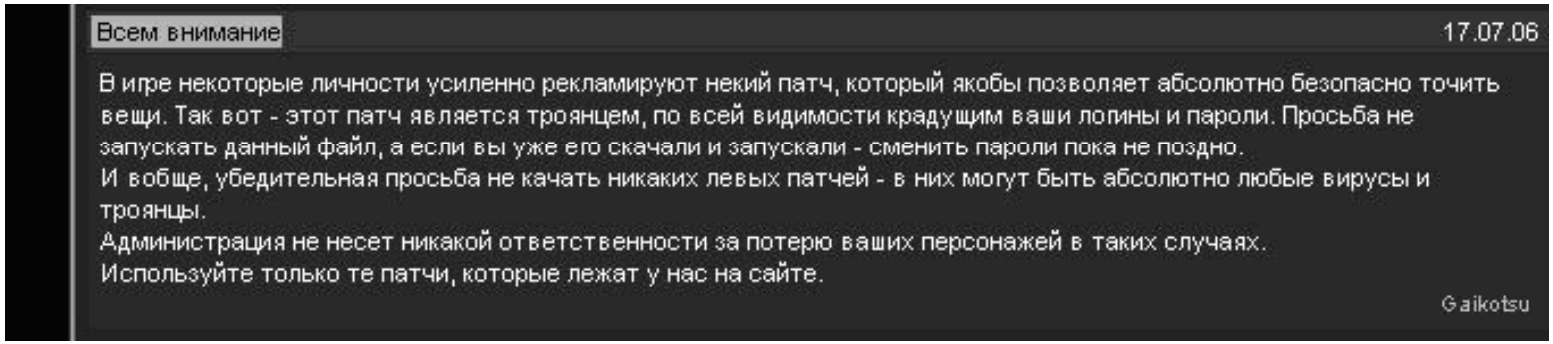
Vulnerability in-Game Chat in Lineage 2

Using Malware

Malicious users create malware and send it using any means possible:

- Publishing links to malicious programs which claim to be game patches on player message boards
- Sending in-game spam containing links to a malicious program presented as a “new patch”
- Sending spam via email with a malicious program attached, or a link to a malicious program
- Spreading malicious programs via file sharing networks
- Exploiting browser vulnerabilities in order to download malicious programs when a user visits a game-related website

Using Malware (cont'd)



Translated, the message above reads as follows:

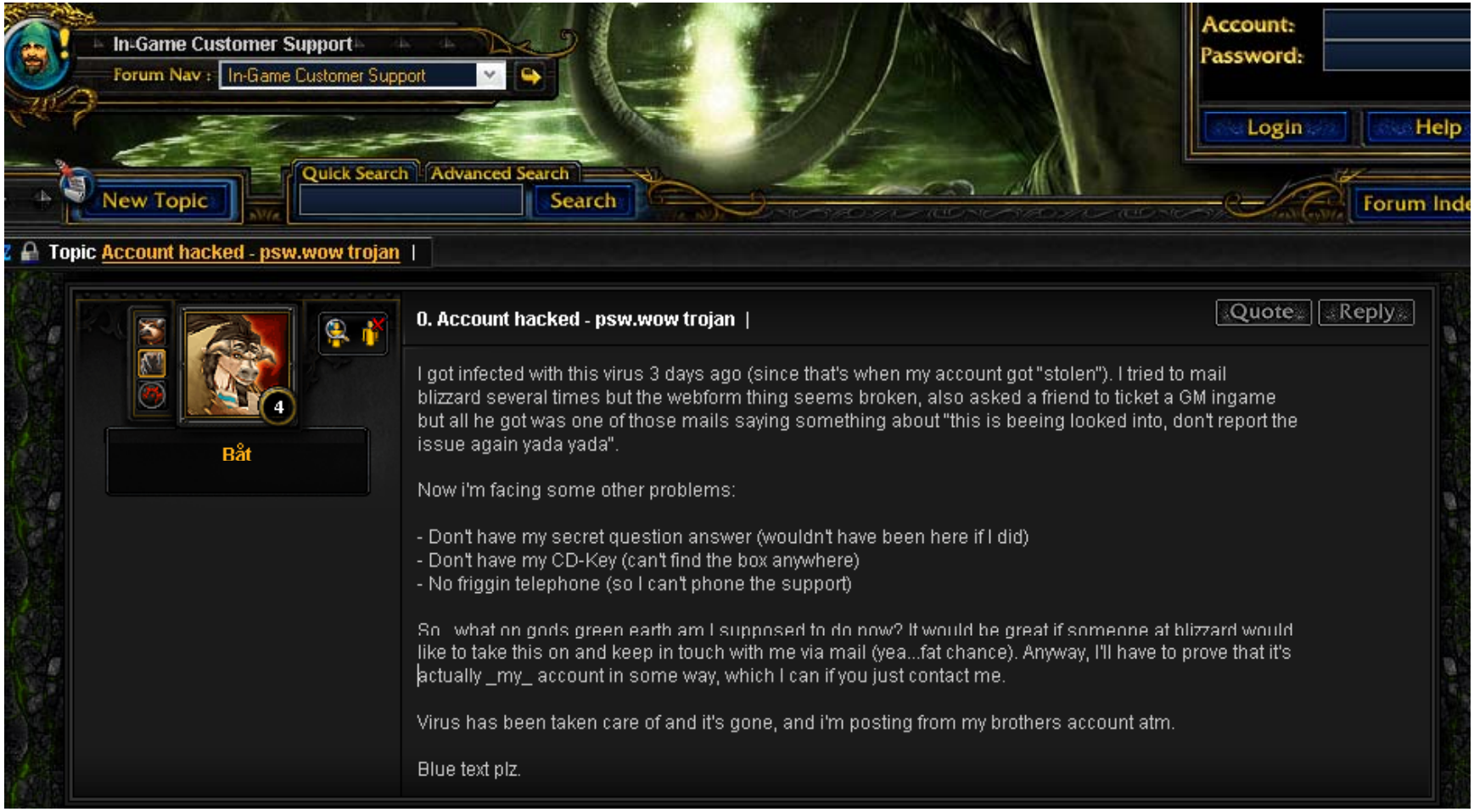
Attention all,

Certain people in this game have been forcefully recommending a certain path, which allegedly makes it possible to enchant items completely safely. This patch is actually a Trojan which steals your user name and password. We ask you not to launch this patch, and if you've already downloaded it and launched it, it's still not too late to change your password. And here's a general earnest request - don't download any dodgy patches because they could contain all types of viruses and Trojans imaginable. In such cases the administrators won't take any responsibility for the loss of your characters. Only use the patches which are on our site.

Malicious Programs and Malware

The following are Malicious Programs and Malware designed to attack online game players:

- Trojan-PSW.Win32
- Trojan.Win32.Qhost
- Trojan-Spy.Win32.Delf
- Trojan-PSW.Win32



Message from a gamer about a password stolen by a malicious program

Email-Worm.Win32.Lewor.a

- The first worm to steal passwords for online games
- This worm sends itself to addresses harvested from Outlook Express address books on infected computers
- If the worm finds user name, password, and server address on an infected computer, it saves that data to an FTP server belonging to a malicious user
- The malware would be designed to copy itself to removable disks with an additional file called “autorun.inf”
- One example of this class of malicious programs is classified by Kaspersky Lab as Worm.Win32.Viking
- Currently, the most recent achievement by those writing viruses for online games is the polymorphic Virus.Win32.Alman.a and its successor, Virus.Win32.Hala.a

Part of a file infected by Virus.Win32.Alman.a

Online Gaming Malware from 1997-2007

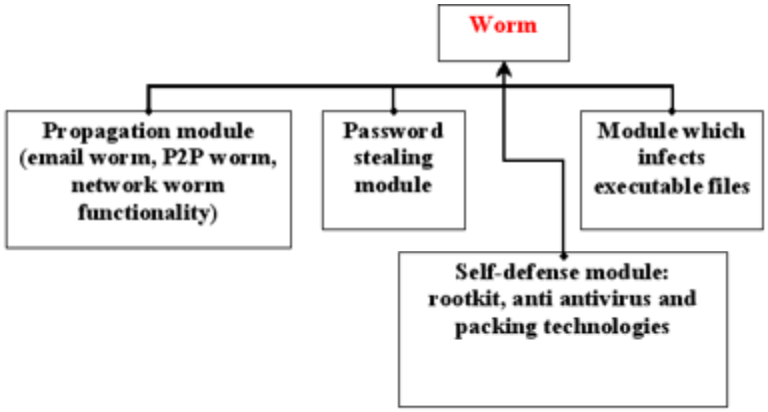
Month, year	Trojans	Worms	Viruses
1997	Classic keyloggers		
2002 December	Trojan-PSW.Win32.Lmir.a		
June 2004		Email-Worm.Win32.Lewor.a	
October 2004	Trojan-PSW.Win32.Nilage.a		
February 2005		Worm.Win32.Viking.a	
December 2005	Trojan-PSW.Win32.WOW.a		
August 2006	Trojan-PSW.Win32.OnLineGames.a		
December 2006		Worm.Win32.Fujack.a	
April 2007			Virus.Win32.Alman.a
June 2007			Virus.Win32.Hala.a

How Modern Attacks are Conducted

Attacks on computer players are conducted by creating worms that have multiple functions:

- Self-replicating (email worms, P2P worms, network worms)
- Infecting executable files (viruses)
- Masking their presence in system (rootkits)
- Stealing passwords (PSW Trojans)

The passwords retrieved after the attack is sent to an email address or to an FTP server on a .cn domain

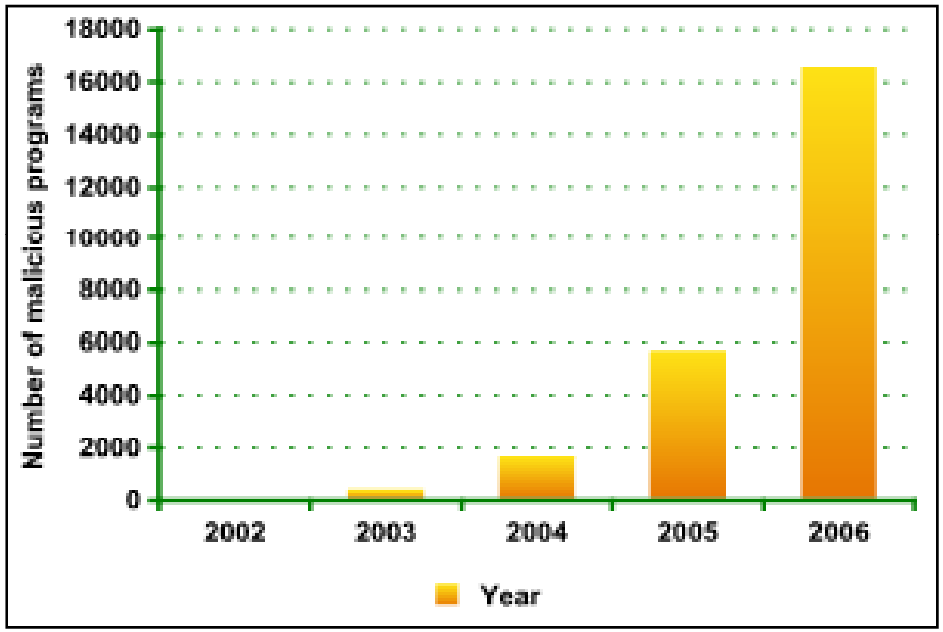


Geographical Considerations

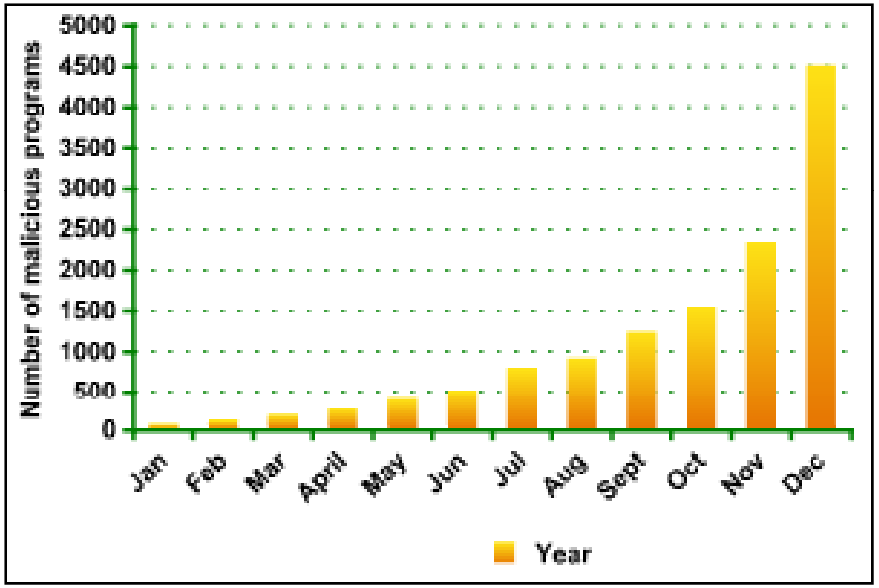
The theft of passwords of online games primarily concerns China and South Korea

The reasons are not entirely clear, but the figures speak for themselves: over 90% of all Trojans targeting online games are written in China, and 90% of passwords stolen by these Trojans belong to players on South Korean sites

Statistics



Total number of malicious programs targeting online game passwords



Malicious programs targeting Lineage 2 and World of Warcraft passwords, 2006

Source: *http://www.viruslist.com/*

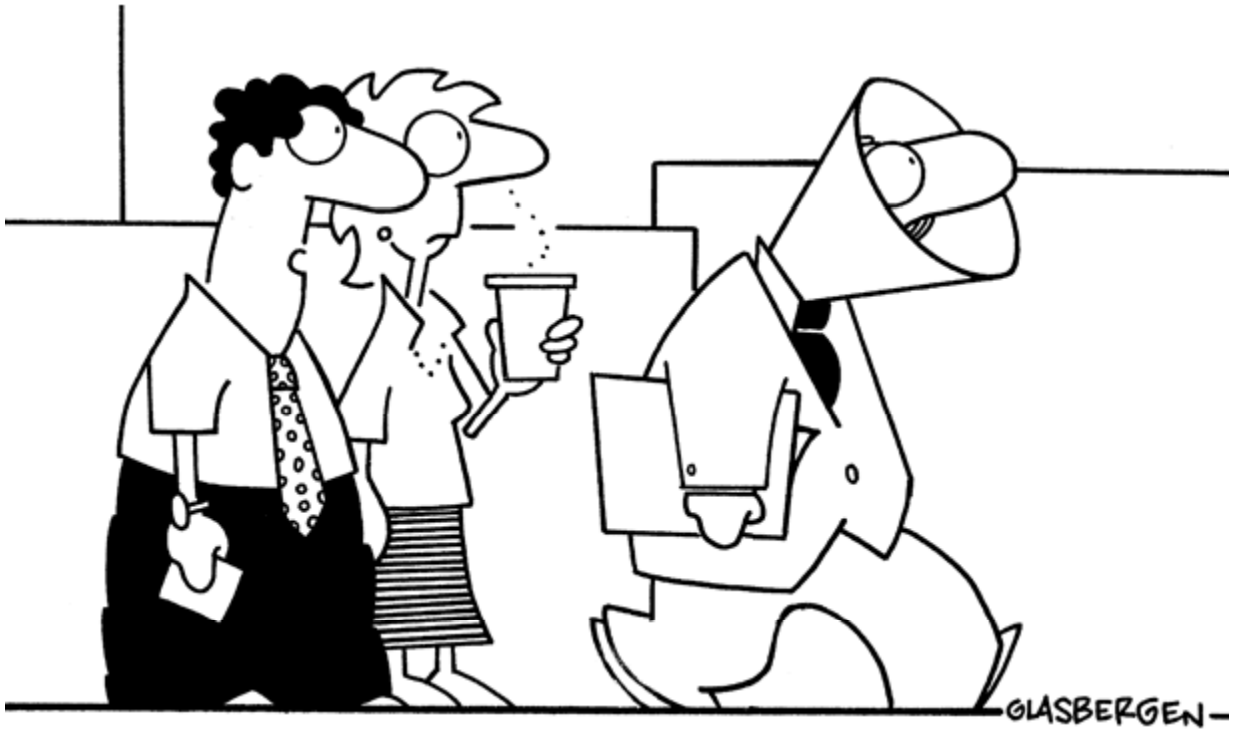
Best Practices for Secure Online Gaming

Steps for protecting Online Gaming from risks are:

- Use antivirus and antispyware programs
- Be cautious about opening files attached to email messages or instant messages
- Verify the authenticity and security of downloaded files and new software
- Configure your web browsers securely
- Use a firewall
- Identify and back-up your personal or financial data
- Create and use strong passwords
- Patch and update your application software

Summary

- Online games are played over a computer network (the Internet) and come in varied forms ranging from simple text based games to games incorporating complex graphics and virtual worlds
- Cheating Massively Distributed Systems, discover the various attacks and hacking techniques to target the vulnerabilities found in online games
- After the theft, malicious users can demand money for stolen items from the users. All online game users are made target by cyber criminals
- Malicious user log on to the machine where the victim is actually playing.
- With online games fast growth and popularity, cheating online games has become a regular incident in current game play on the Internet
- Cyber criminals steal only the user name and passwords of victim users, and not the address of server where the user is actually playing the game.
- Game Servers comes with system services, programs and databases designed to support on line games



"He lost a lot of money on Wall Street. The plastic funnel keeps him from licking his wounds."

"I don't invest online anymore. I could never tell if the stock market was crashing or just my computer."