

# Playing Dirty: Evolving Security Threats in the Gaming World

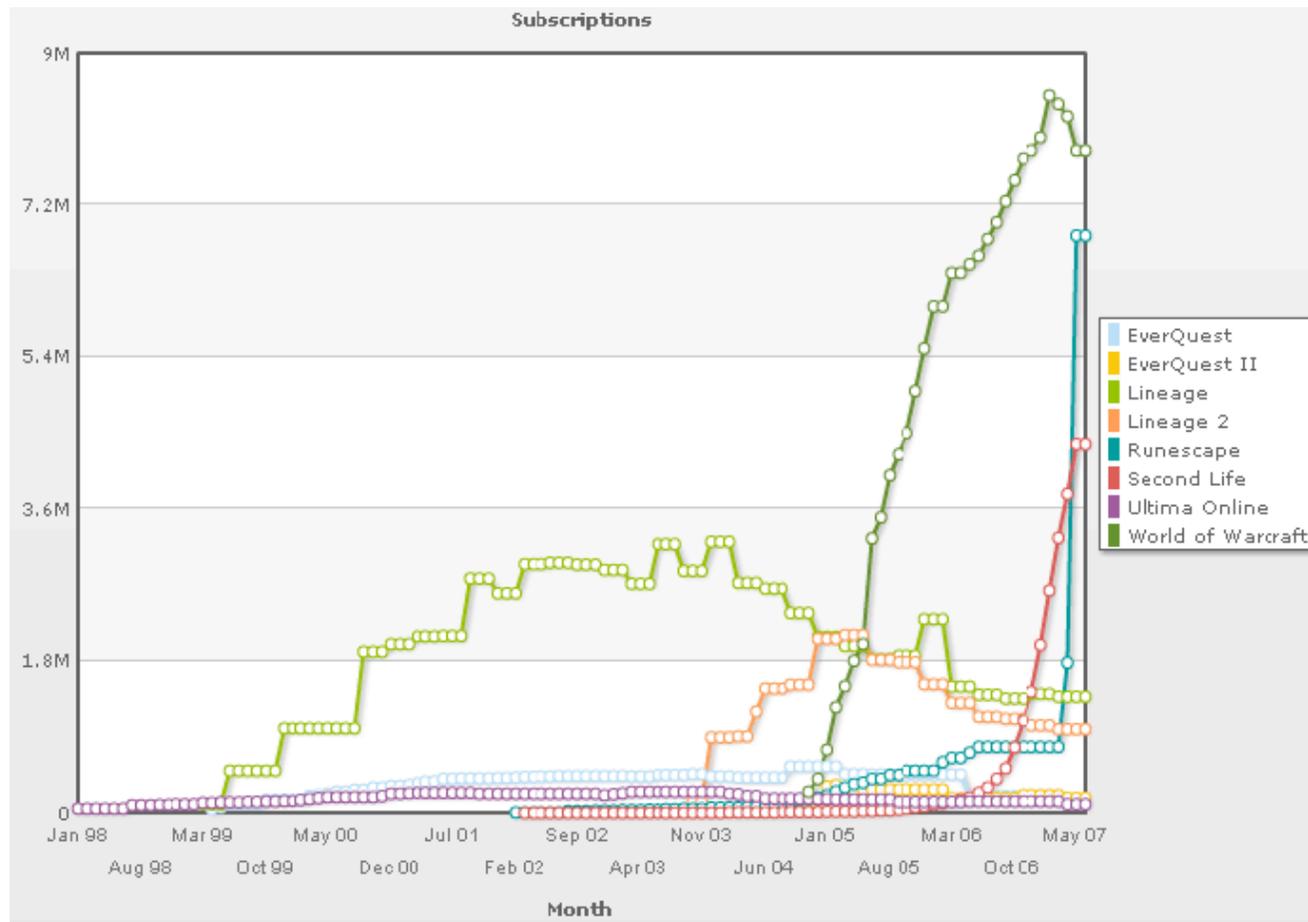
Amir Fouda and  
Hannah Mariner, CA

# MMOR-thingamijig?



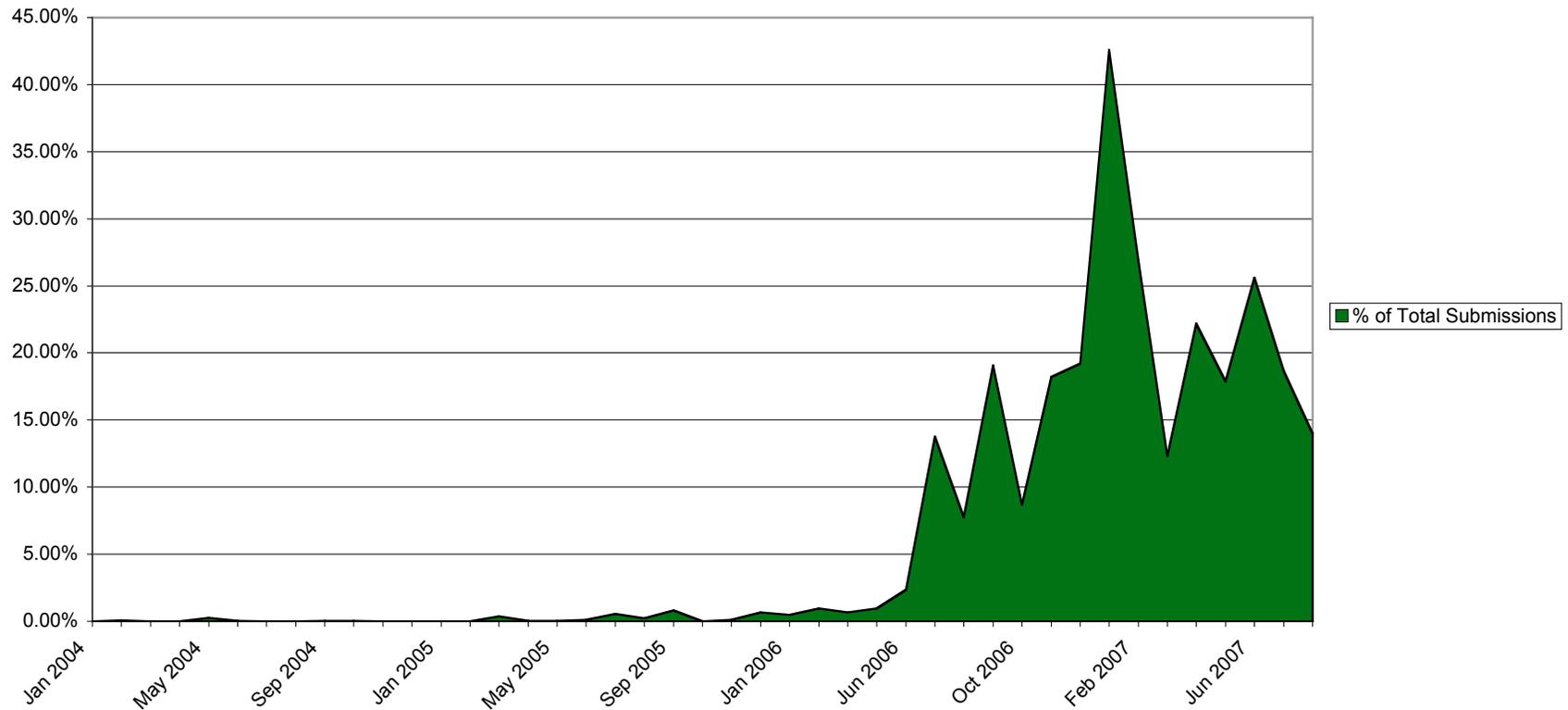
**M** assively  
**M** ultiplayer  
**O** nline  
**R** ole  
**P** laying  
**G** ame

# MMORPG subscription growth 1998 - 2007



Source: <http://mmogdata.voig.com>

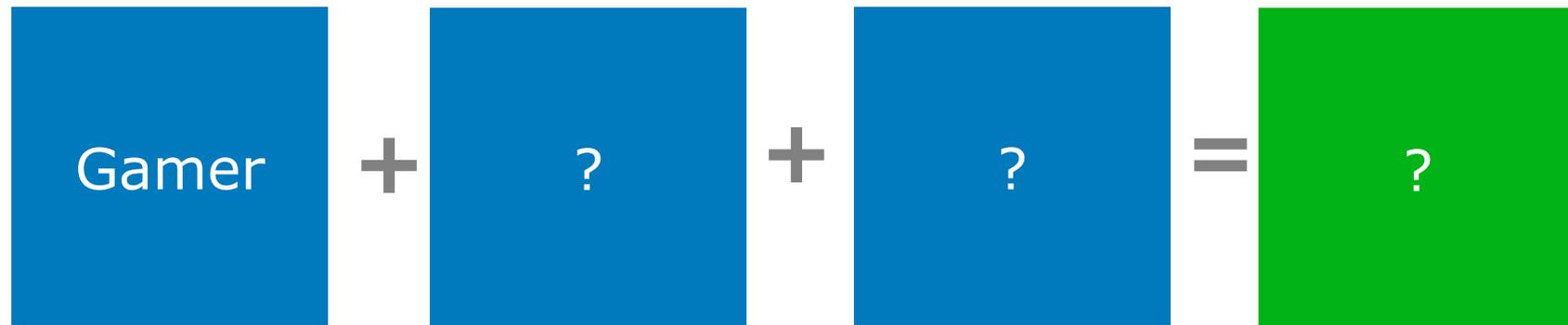
# Game-targeting malware growth 2004 - 2007



Source: CA Anti-Virus Research Labs



# You haven't told me what a gamer is!



> Most gamers put significant time into playing an MMORPG and related activities

- In-game: collecting currency, buying supplies, training in a trade, building skills, establishing friendly connections
- Out-game: visiting forums, gamer websites, developer websites

# Virtual goods bought with real money!



> The crossover of virtual and real economies

# Currency selling for...



WoW	100 Gold = US\$12.82
Lineage II	30 Million Adena = US\$16.55
EverQuest	20 Platinum = US\$24.86

**Rates retrieved August 2007**

# Accounts selling for...

## Final Fantasy XI – Red Mage, US\$1299

75



Red Mage

Midgardsormr

Not Ranked  
[View Gear](#)

75 Female Mithra  
Summoner/75 White  
Mage/75 Black  
Mage/75 Red Mage! All  
Avatars, Zil/Prom  
Complete! 700K Gil &  
More!

\$1299

BUY  
NOW

## EverQuest II – Bruiser, US\$699

70



Bruiser

Befallen (evil)

Not Ranked  
[View Gear](#)

70 Male Dark Elf  
Bruiser / 55 Tailor With  
Awesome Gear, Tons  
of Fabled & A 60  
Barbarian Warrior!

\$699

BUY  
NOW

## World of Warcraft – Mage, US\$1199

70



Mage



Ysera US (Normal)

★★★★★  
[View Gear](#)

\* Level 70 Undead Mage With  
Awesome Gear, Mixed Epic &  
Rare Items, EPIC NETHERRAY  
& NETHERDRAKE & Tons Of  
Extras! MUST HAVE!

\$1199

BUY  
NOW

\* Includes A Level 63 Rogue!

Example rates retrieved from <http://www.accounts.net>, September 2007

# Known as the Real Money Trade (RMT)

- > RMT refers to exchange of real money for virtual goods
- > Malware authors, highly motivated by the opportunity to profit, use malware to obtain stolen accounts and goods that can then be resold for real profit



# What do gamers really want?

- > MMORPGs typically offer gamers a “rags-to-riches” experience
- > *“Getting a bunch of characters to 70 is a pain. Getting money to equip them is a pain... We use the Glider to skip the painful parts and have more fun.”* MMO Glider website



So far, this is interesting but not security relevant...

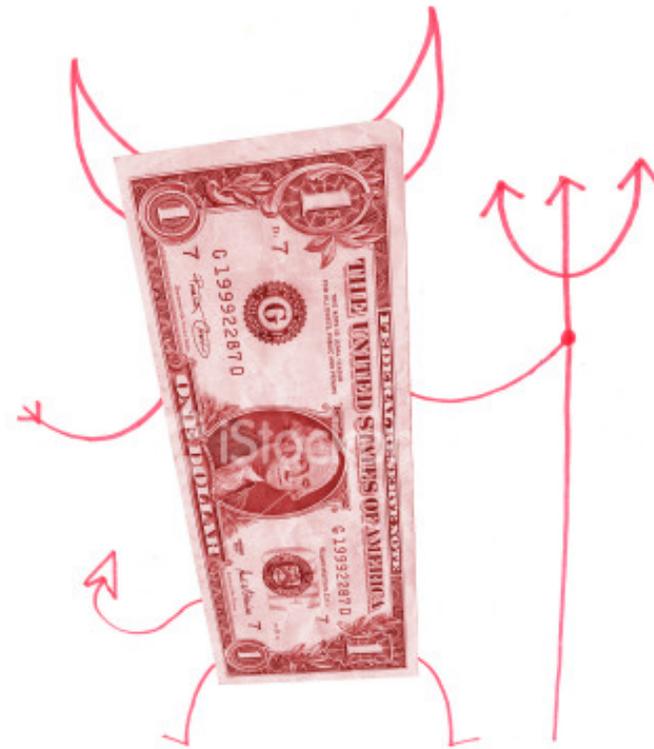


> This is the point where the financially motivated malware author can prey on and exploit a gamer's desire to progress in the game with less manual effort

## What's in it for a malware author?

# Money

- > Malware authors almost strictly profit-motivated
- > More than 30 million estimated MMORPG subscribers regularly spending money on access to virtual worlds



Just money or something else too?

Notoriety  
Revenge  
Fun

- > Emerleox (alias Fujacks) malware author told various sources he wanted to have some fun and also wanted revenge on IT organisations who did not hire him
- > (He also sold Emerleox and variants to 12 people, earning US\$12,500)

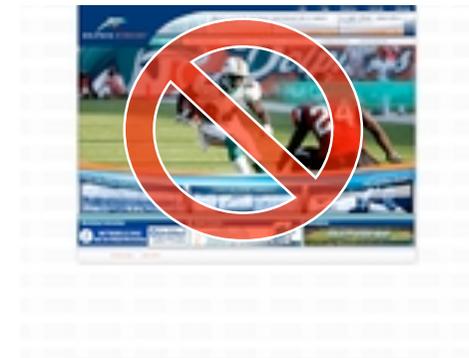
# Using the user



- > Social engineering enables an attacker to manipulate users
- > Different traps laid to catch users of various abilities, from the novice to the savvy

# No patch, no trust

- > Hacking into websites and planting malicious code is a common way malware writers deliver game targeting malware to systems
- > Using techniques such as SQL injection, exploit code or links to exploit-ridden websites can be inserted into the main pages of these compromised sites



# What you see is not what you get

- > Malware can be disguised as legitimate programs or third party applications
- > Luring the oblivious, the curious, and the ambitious



# Fooling the gamer

- > Downloaded from unofficial gaming websites and/or fraudulent websites
- > Downloaded via links posted on gaming forums
- > Circulated through in-game chat and through emails

The screenshot shows a website designed to look like the official Nokia site. It features the Nokia logo and 'Connecting People' tagline. The navigation bar includes links for 'Home', 'Mobile Phone', 'Partners & Support', 'Enterprise Solutions', 'Service Network', 'Investor Relations', and 'About Nokia'. The main content area is titled '歡迎光臨諾基亞台灣網站' (Welcome to the Nokia Taiwan Website). It displays several promotional banners for Nokia products, including the 'L'Amour Collection' (Nokia 7360, 7370, 7360), 'Nokia N70' (described as the smallest 3G smartphone with 200MB memory and internal camera), 'HS-55W 無線耳機' (HS-55W Wireless Earphone), and a 'Club Nokia' membership recruitment banner. There are also sections for '服務與支援' (Service & Support), '最新活動' (Latest Activities) featuring a promotion for Nokia 6270, and a '新聞中心' (News Center) with a link to '外型迷你 內在迷人' (Mini外形 內在迷人). The website layout and content are highly detailed and professional-looking, mimicking the official Nokia site.

Fraudulent Nokia site Source: <http://www.websense.com/securitylabs/alerts/alert.php?AlertID=441>

# What about the malware itself?

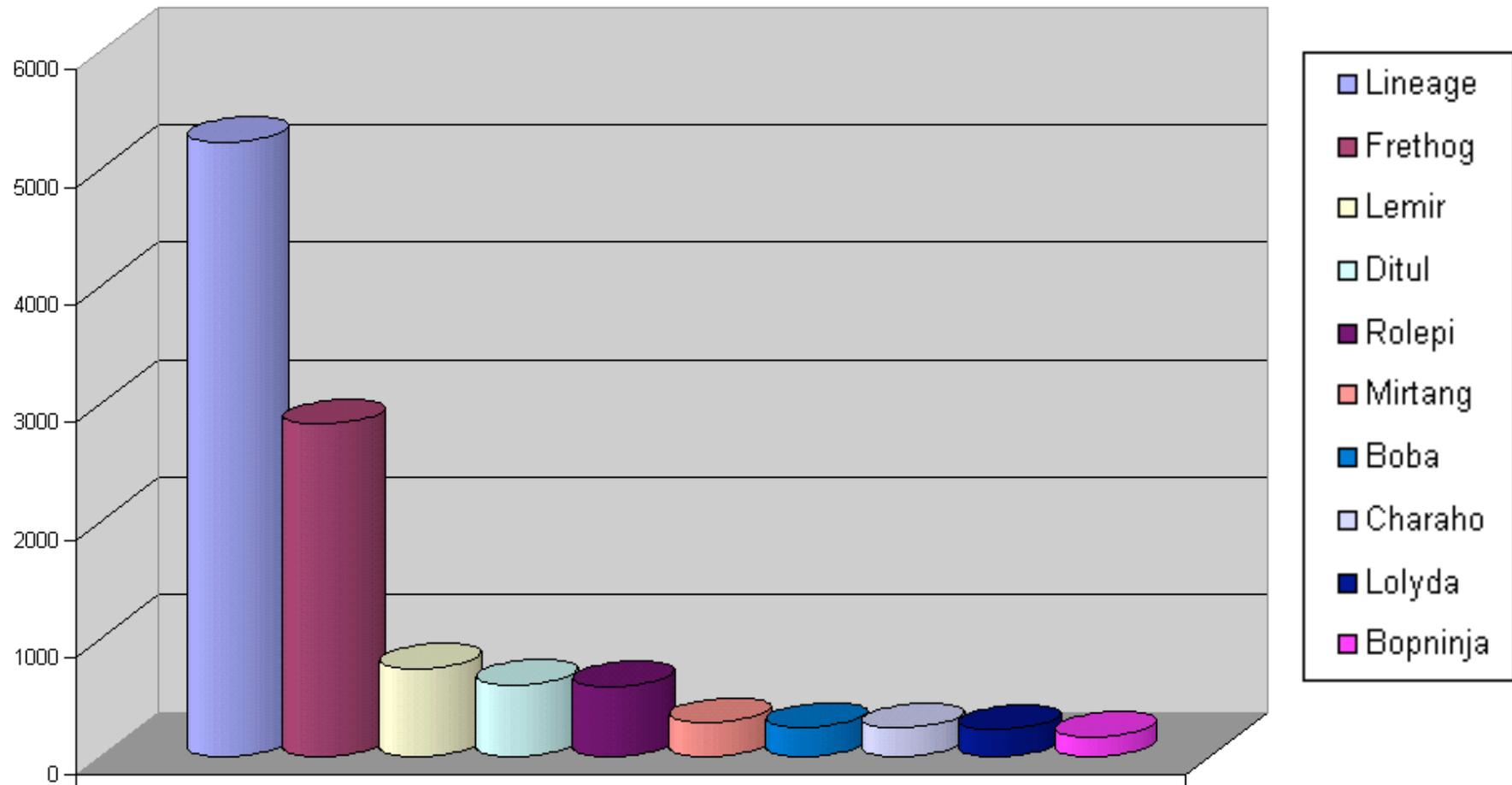
- > CA Anti-Virus Research labs have classified over 45 different malware families that target MMORPGs
- > 80% of these are information stealing trojans that contain keylogging and/or data gathering capabilities



# Game information stealing trojans

## Top Ten families

Number of Samples



# Face the facts

- > Three of the most targetted MMORPGs are Lineage II, Legend of Mir II and World of Warcraft
- > Win32/Lemir was one of the earliest game information stealing trojan families to emerge
- > Many of these trojans originate from China
- > No coincidence that many MMORPGs originate from and are extremely popular in East Asia

# What game do these trojans play?



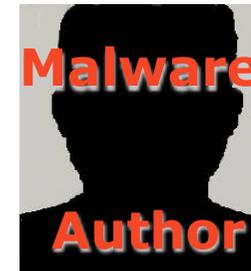
**Downloaded  
onto system**



**System  
activity  
monitored**



**Game  
information  
logged**



**Information  
dispatched**

# What information is logged?

> Username and password

> In-game information

Level

Currency

Role

Occupation

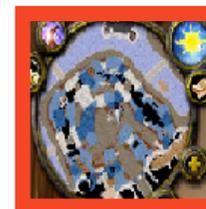
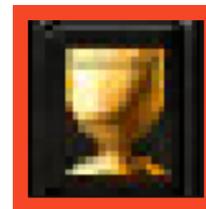
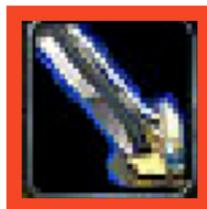
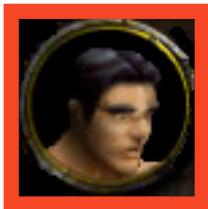
Server name

Location

Character

Equipment

Items



# Sending the information to the author

- > Gathered information can be stored in a log file on local machine
  - Attached to an email and sent to a pre-determined email address
  - Uploaded to a web server via HTTP
- > Malware can construct a specially crafted URL containing stolen information
  - Posted to a web server to be processed by a server side script

# Dispatching the information

The screenshot shows the 'Legend of Mir Sniffer v6.02' interface. The main window displays a captured packet with the following details:

- From:** 传奇截密者
- Date:** Monday, 8 December 2003 6:32 PM
- To:** 8018860.com
- Subject:** 传奇截密者v6.02

The packet content is as follows:

传奇登录

区域: -----

用户名: testing un

密码: testing pw

服务器: testing sp

角色: testing ch

附加信息

-----

IP地址: 192.168.226.129

计算机名: KETEST

发送时间: 2003-12-9 12:32:46

欢迎注册传奇截密者 <www.18600.net> QQ: , E-Mail: @163.com

Labels and their corresponding fields:

- Username:** testing un
- Password:** testing pw
- Server Name:** testing sp
- Character:** testing ch
- I.P.:** 192.168.226.129
- Computer Name:** KETEST
- Time:** 2003-12-9 12:32:46

# Casting a wider net

- > Traditional file infectors and worms have been used by malware authors to compromise further systems
- > Win32/Looked and Win32/Emerleox (alias Fujacks) are among the more widespread file-infecting worms found in the wild in late 2006, early 2007
- > Both capable of spreading through network shares and downloading game information stealing trojans onto compromised systems

# Win32/Emerleox (alias Fujacks)

## > Contains multiple avenues of attack



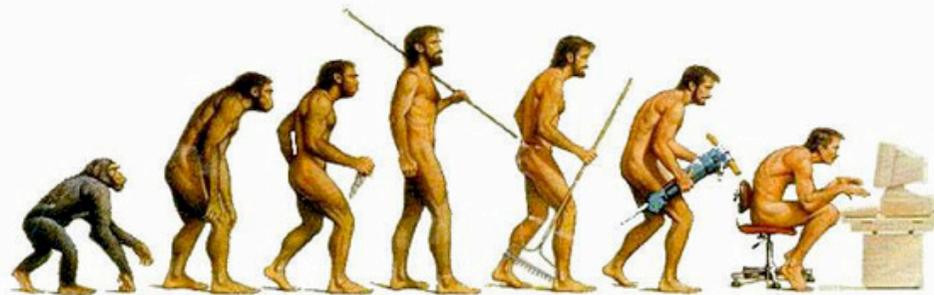
- Infects executables (exe, scr, pif, com)
- Appends IFRAME to scripts (html, htm, asp, php) that points to a malicious website
- Spreads through network shares and removable drives
- Downloads file containing list of URLs that point to other malware (including updates of the worm or game information stealing trojans)

# Win32/Looked

- > Similar to Emerleox, it infects executables and spreads through network shares
- > Downloads a large number of game information stealing trojans onto a system
- > Some variants have been observed to download up to 20 trojans onto a system
- > Downloaded trojans include game information stealing trojans that target various MMORPGs such as World of Warcraft, Lineage, Legend of Mir, Zero Online, Ultima Online

# How they have evolved

- > Self-replicating, file infecting, downloading
- > Use of encryptors and packers
- > Use of process injection to obfuscate activity



# Do we know how to keep gamers and their machines safe?



## > Role of:

- Game developers
- Gaming community
- Anti-Virus Industry



# Conclusion

- > Game targeting malware has caused strife to gamers and game developers alike
- > Game targeting malware will continue to cause havoc as long as the popularity of MMORPGs remains high
- > If there is demand, malware authors will deliver



# Questions?



[amir.fouda](mailto:<amir.fouda><hannah.mariner>@ca.com)<hannah.mariner>@ca.com