# Security in MMORPGs

Presented by:

Will LaSala

Director of Services, US

VASCO Data Security, INC.

Game Developers Conference
Austin, TX
September 17, 2008

# Who am I?

- I am MrTaz20 lvl 40 Barbarian in my Dial-up Dragon's Gate MUD in 1996

- I am Iweil a lvl 60 Wood Elf Ranger of Tunare on Povar in 2002

- I am Iweil a lvl 60 Nightelf Warrior on Bloodhoof in 2005

- I am Iweil a lvl 70 Dwarf Hunter on Dark Iron now

- Implemented Online security measures in 85% of the top 100 banks around the US

- Developed dozens of security applications for ISPs and ASPs

# Synopsis

- We've heard this before, what's different about security in MMOG's this time?

- Why do we care about this now?

- What types of security concerns are their for MMORPG's?

- Why focus on Account theft first?

- How are the big bucks being made?

- What forms of Account Security are out there?

- How much work does fixing your games security take?

- How will making my game secure bring me more subscribers?

# What's New about Security in MMOG's?

- Other industries are becoming harder to attack

- The destruction and erosion of gaming economies has become a flourishing mainstream industry

- Viruses and other Malware attacking gamers are on the rise

- Hackers and Thieves in the virtual worlds are now facing real world prosecution
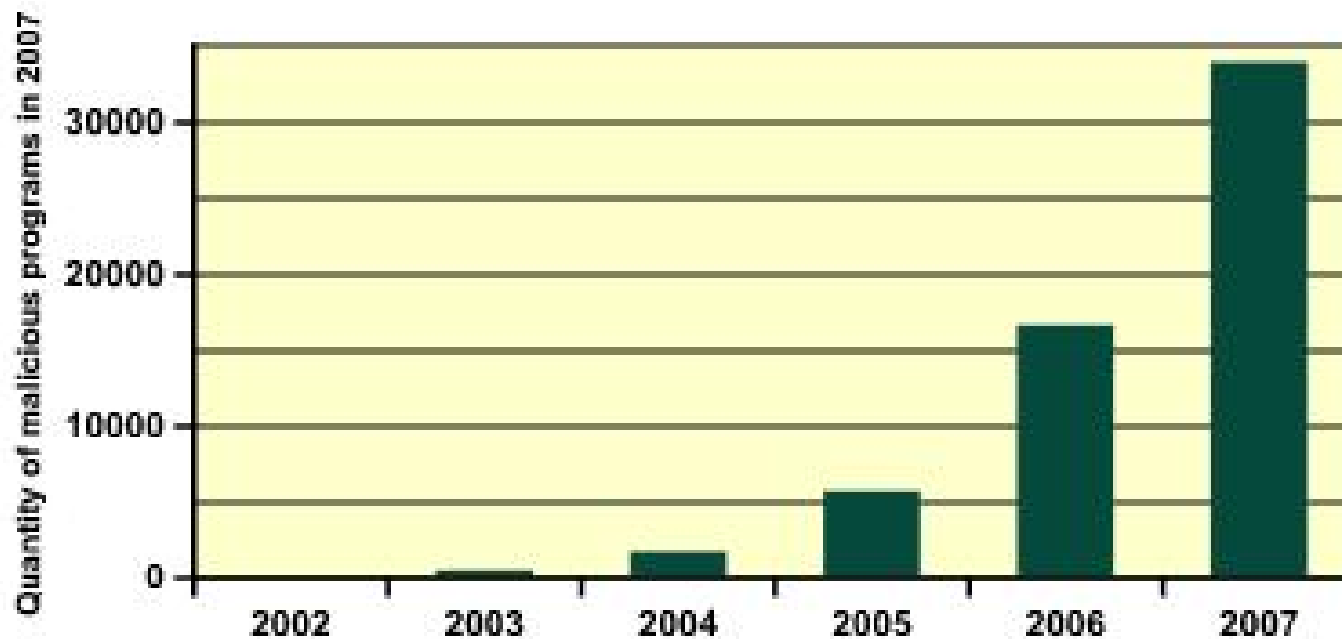
## Rise of Malware focused on MMOG's

In a report posted online at:
http://www.viruslist.com/en/viruses/analysis?pubid=204791985

**Sergey Golovanov of Kaspersky Labs states that,** "In 2007, the number of malicious programs which only target online game players increased by **145%** from 2006."

# Profile of your Players

Why are they still playing?

- Fun

- Relaxation

- Risk vs. Reward

- Real world social impacts

- Improves their job performance...?


Security wasn't considered necessary...

These are GAMES right?!?

# Security Threats and MMOG's

- Summarized (You've heard this before)
    - Bugs
    - Software Hacks
    - Network Hacks
    - Account Attacks

## Security Threats - Bugs

# There are no bugs, we are perfect.

- Who's attacking?

  - Often your strongest gamers and guilds

- How often are they found?

  - Well since there are none, they are never found

  - or at least not till the next patch.

- Exploits take time to discover

- Who's taking advantage of the problem?

  - Mainly hardcore gamers or friends of the exploiter

# Security Threats – Software Hacks

- Who's attacking?

    – Developers with too much free time

- How often are they found?

- Exploits problems in general game designs

    – We tend to reuse code that works

    – MMOG's are generally designed the same way

    – There maybe changes coming

- Who's taking advantage of the problem?

    – Potential to distribute to a wide audience if not resolved quickly

# Security Threats – Network Hacks

- Who's attacking?

  - IT people with free time

- How often are they found?

- Exploits in general computer and network technologies.

  - Redirecting packets

  - Attacking Databases

  - Remote Control of PC's

- Who's taking advantage of the problem?

  - Distribution can be to the same audience as software hacks if not fixed in time.

# Security Threats – Account Attacks

- Every computer user is potentially attacked every day
  - Gamers
  - Politicians
  - Developers
  - Web Surfers

- Attacks are standard, they haven't changed since the days of the Melissa Virus

- Move from industry to industry focusing on the hottest and biggest yield ones first
  - Banking has been the most focused on...
  - But the world has noticed and things are tougher for the attacker
  - Virtual Economies are on the rise. Industries to support these economies are gaining market shares

# Anatomy of an Account Attacker
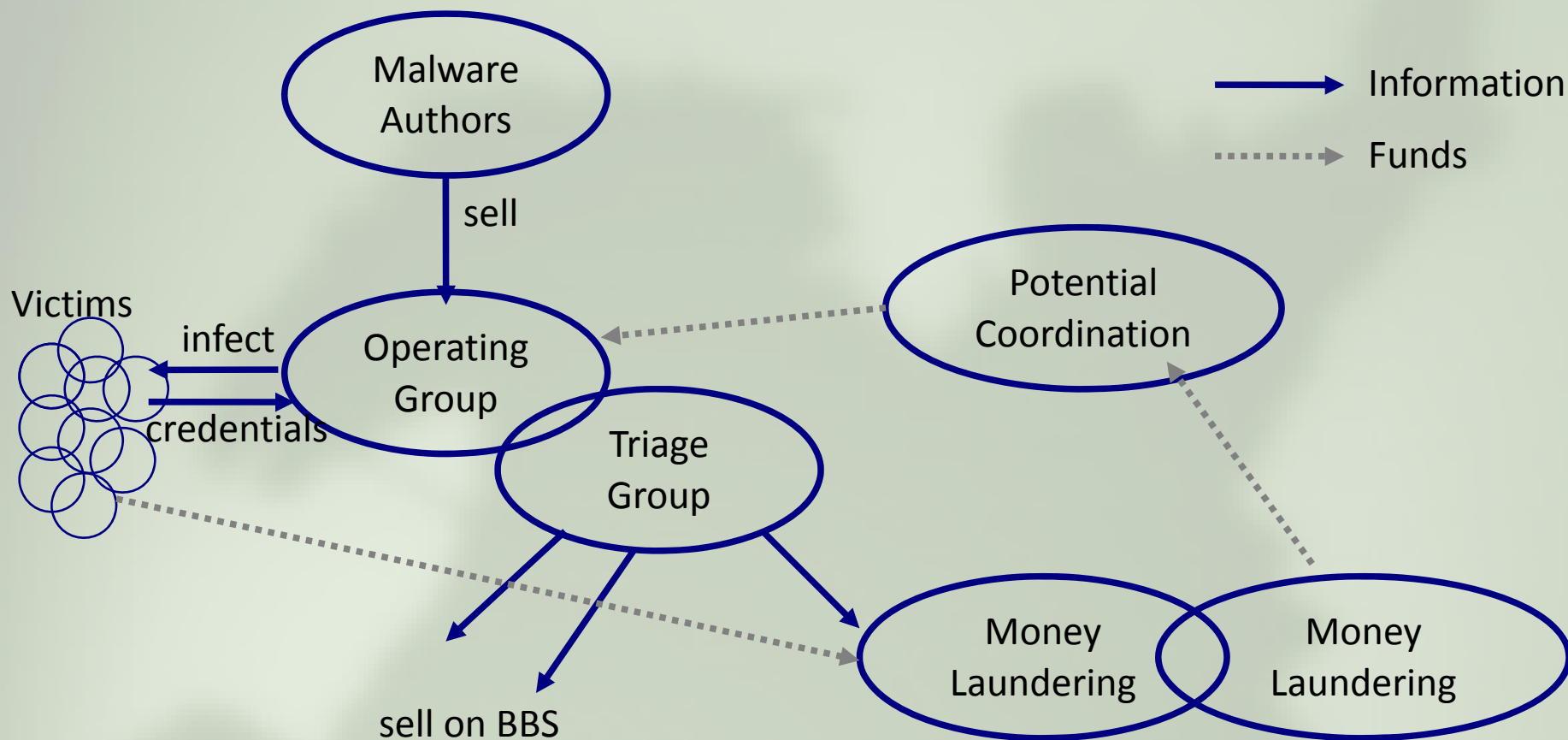
# Protecting your Users

- Static Passwords

- Client Side Software

- User Behavior Analysis

- Mobile Software

- Hardware Tokens

- Hardware Dongles

- Certificates

- Biometrics
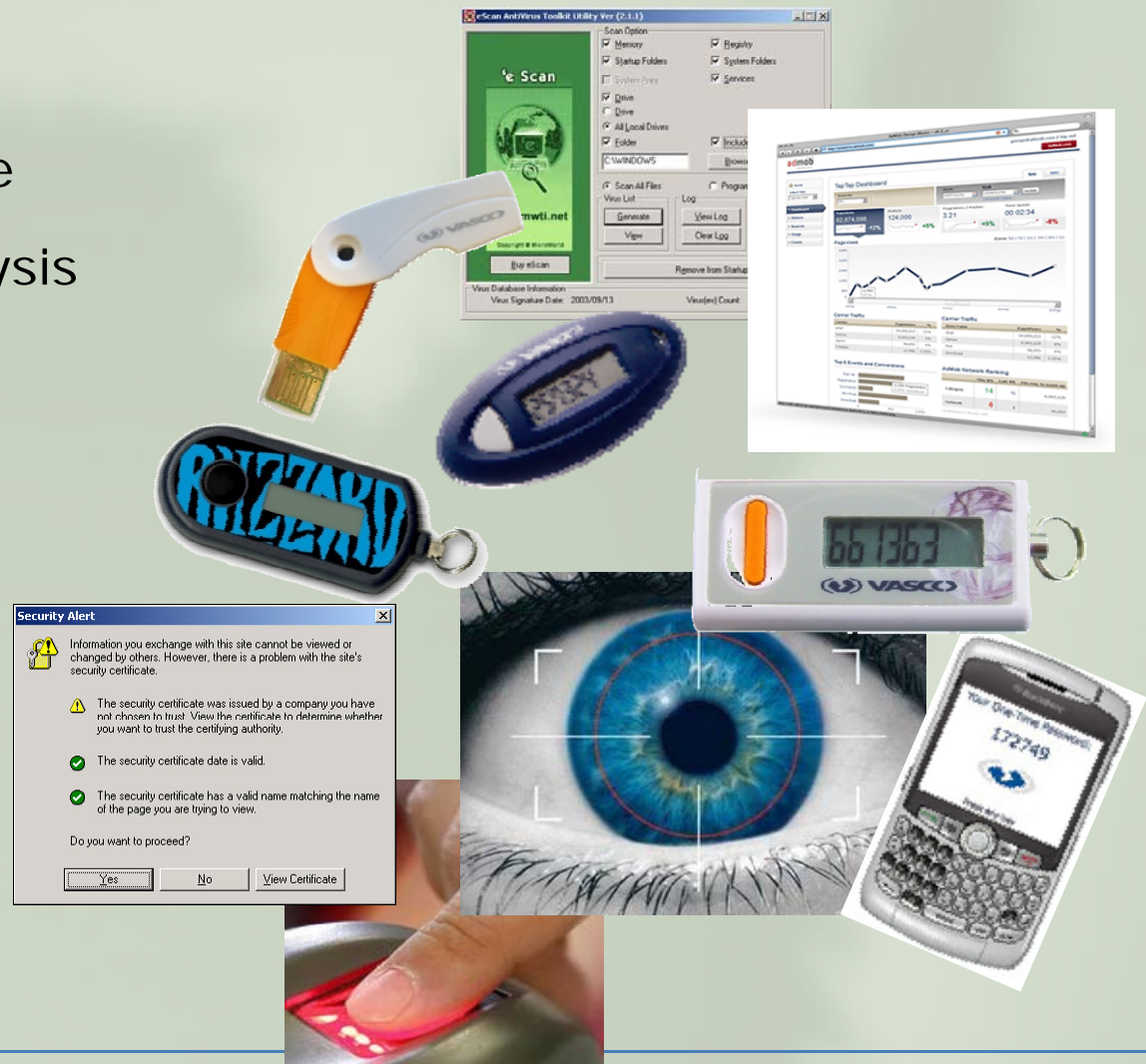
# How to protect your game

- Which option is right for us?

    - Does it impact your users?

    - Will your users use it?

    - How much time does it take to get running?

        - Server Side

            - API or New Server Structure

        - Client Side

            - Deployment

# Secure Users = Happy Users

- Users that have been hacked lose interest in your game

  – Typical response time is 2 weeks to repair an account

- Accounts that have been hacked cause virtual economic damage

  – Thousands of in game denominations can be made by guessing a users password

- Accounts that have been hacked cost you money

  – Forum Moderators

  – Database Programmers

  – Helpdesk Personnel

  – Customer Service Groups

  – In-Game Support

# Conclusion

- Hacking users is the easiest type of attack

- Account stealing is profitable

- There are many options out there

- Customers need simple security

- Keeping customers = increasing their security