Playing with shadows - exposing the black market for online game password theft

Chun Feng
Microsoft Malware Protection Center, Australia
chun.feng@microsoft.com

“Trojan writers drive BMW”

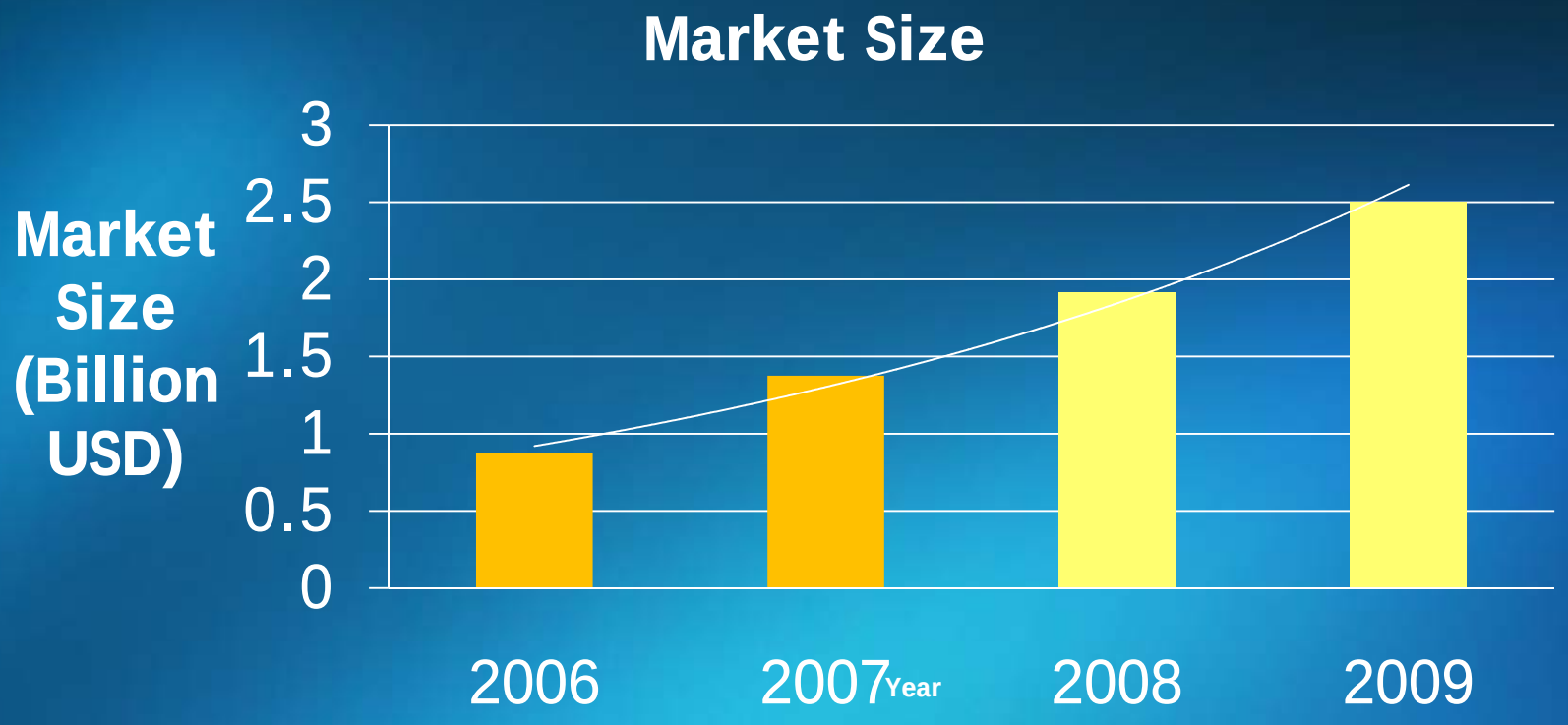
写木马，开宝马

Unprecendented Success of Online games

- WOW (World of Warcraft) reached 10 million users worldwide by Jan 2008
- Online game users in China reached over 40 Million by December 2007

Examples of popular online games

Fast Growth of Online Games market in China



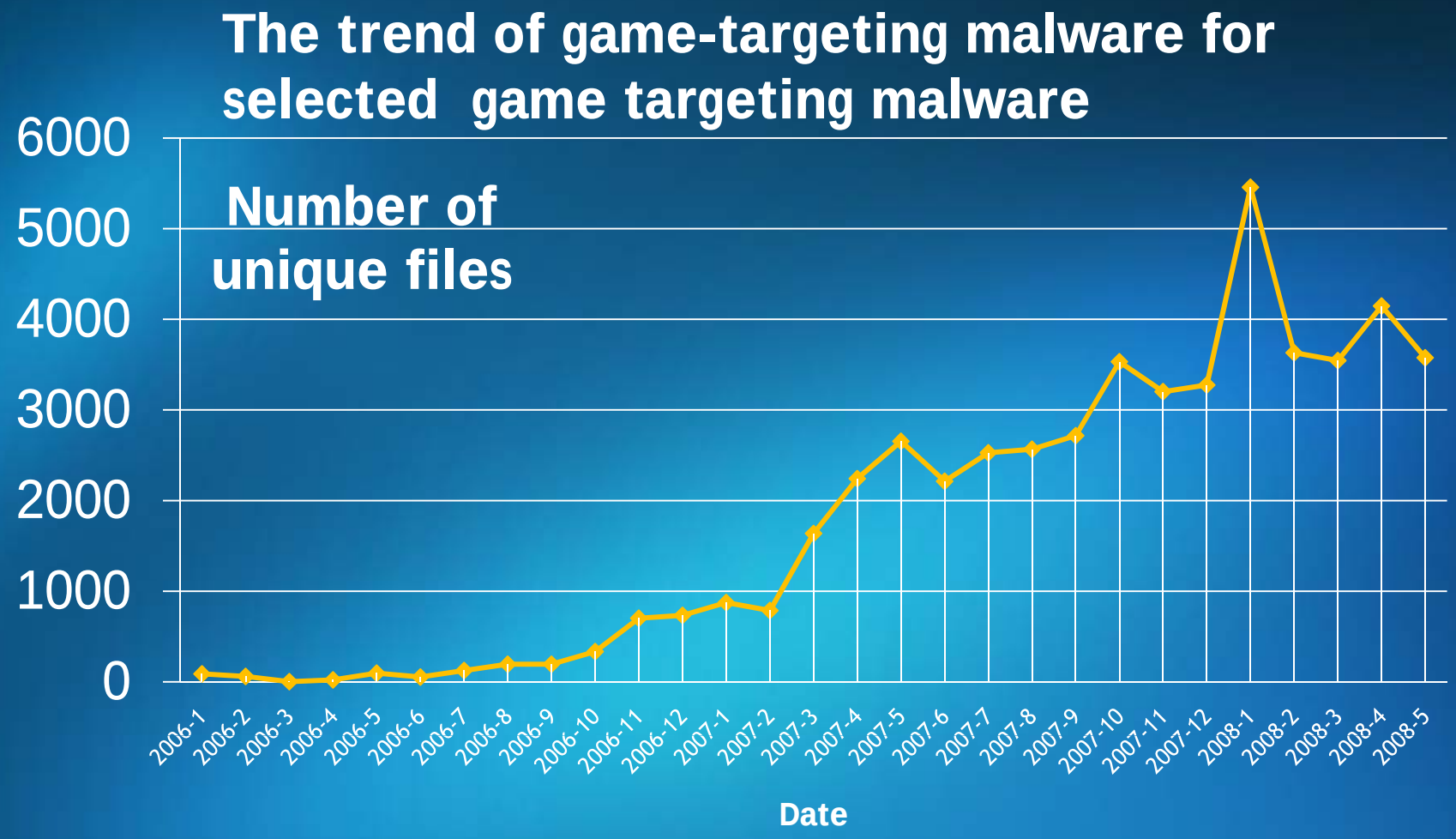
Statistical data from DCCI (Data Centre of CHINA Internet)

Online games account is real money

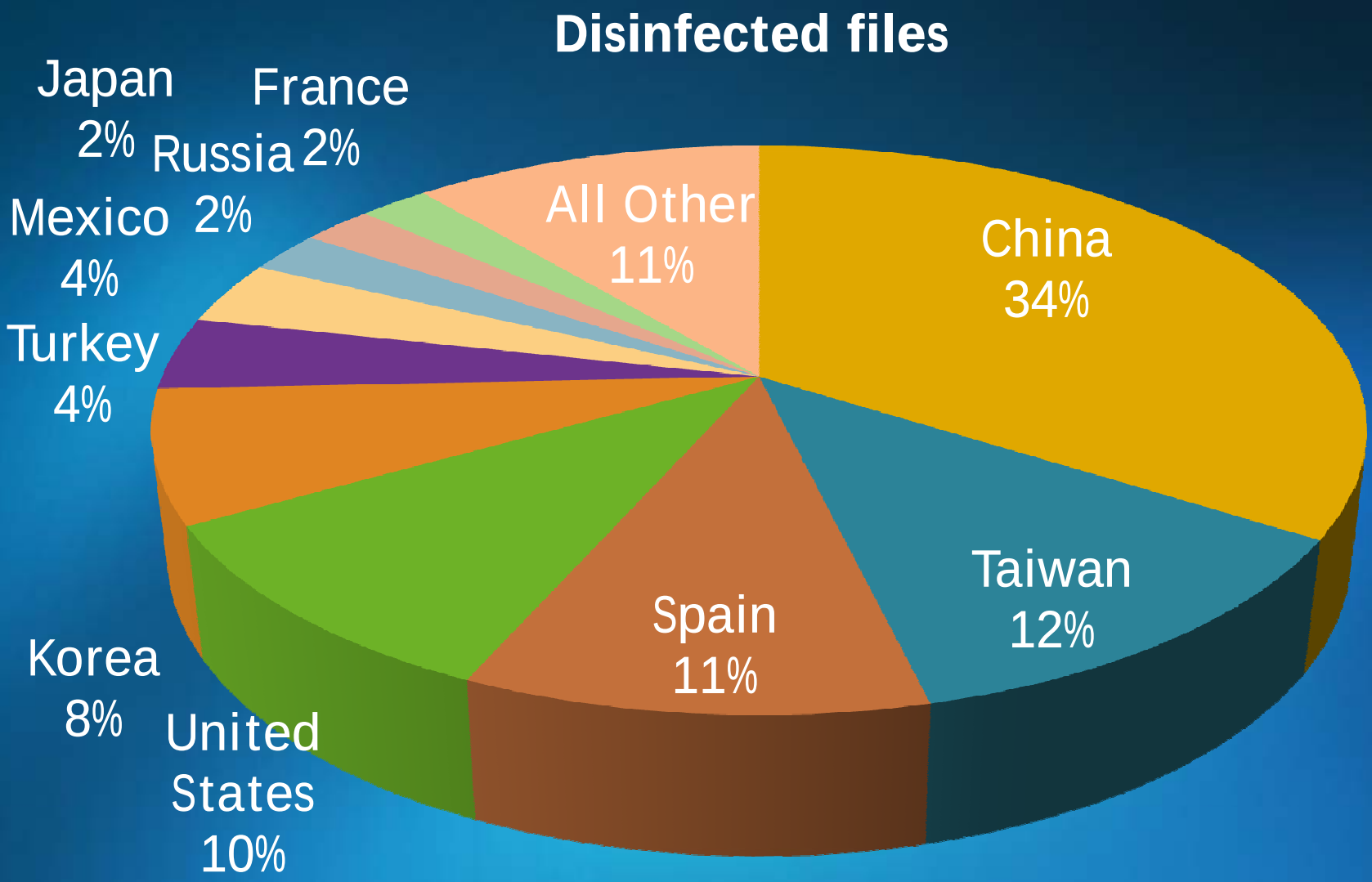
Virtual account contains:

- Level – Time = Money (WOW Level 70 = 360 hours)
- Virtual Object – large demand for remarkable virtual objects (rare item = $1500)
- Virtual Money – Can be potentially converted to real money (1000 WOW gold = $30-$40)

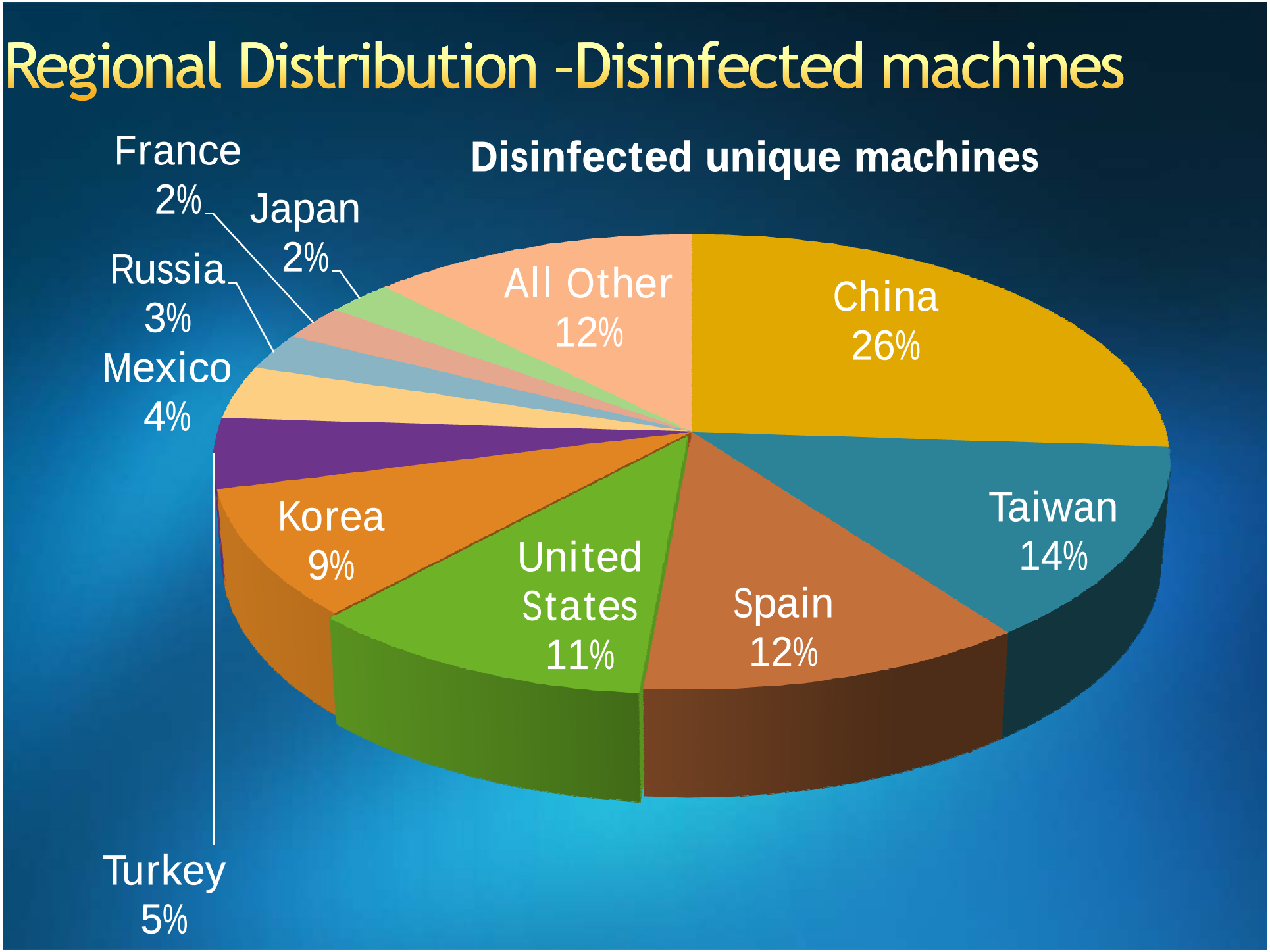
Online games account becomes the target of malware



Regional distribution -Disinfected Files



Regional Distribution -Disinfected machines



What is Market

Any structure that allows buyers and sellers to exchange any goods, services, and information

- Products
- Buyers
- Sellers

Products on the black market

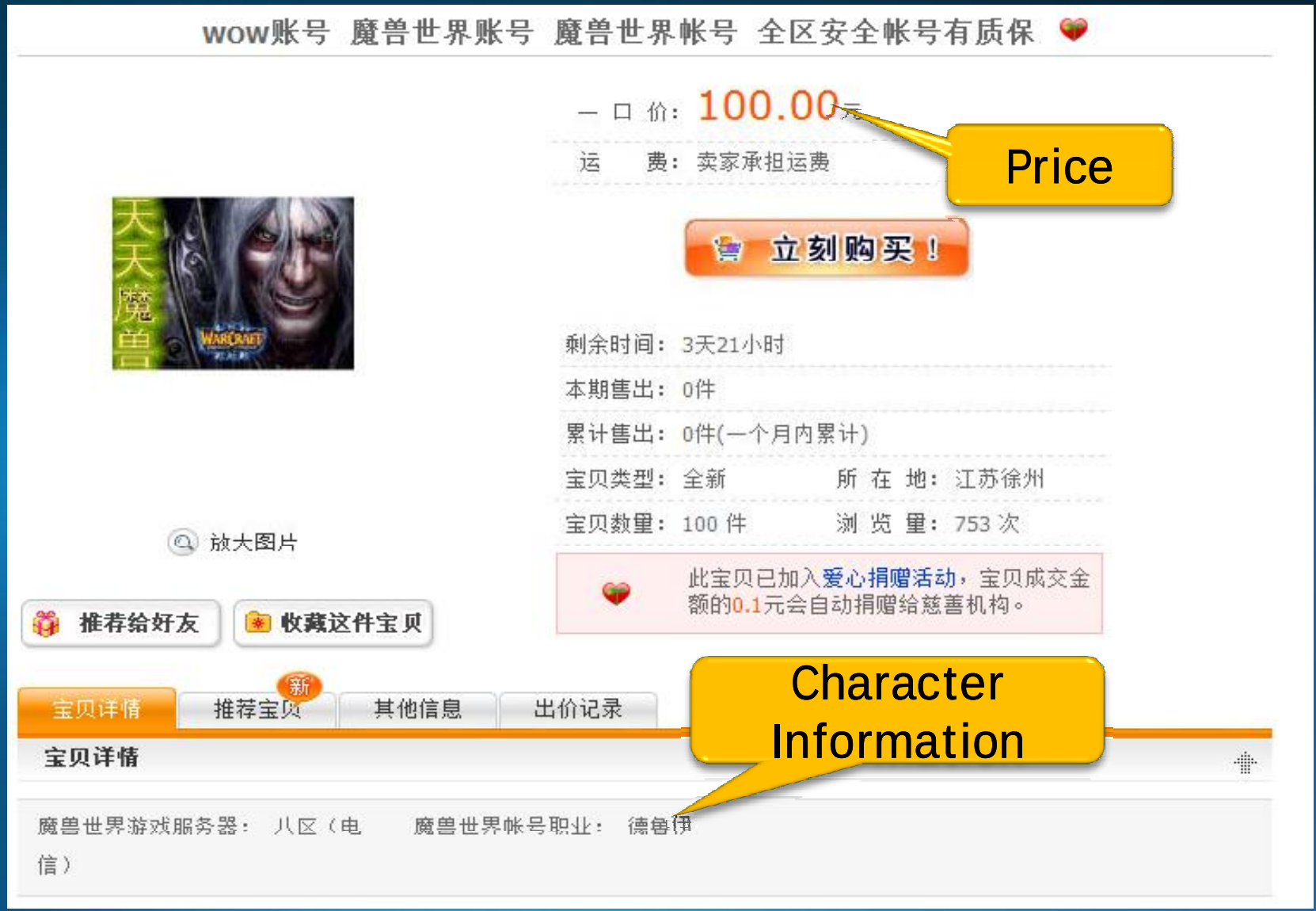
- Envelopes
- Stalls
- Trojans
- Trojan Generators

Envelopes

The account information stolen from online games

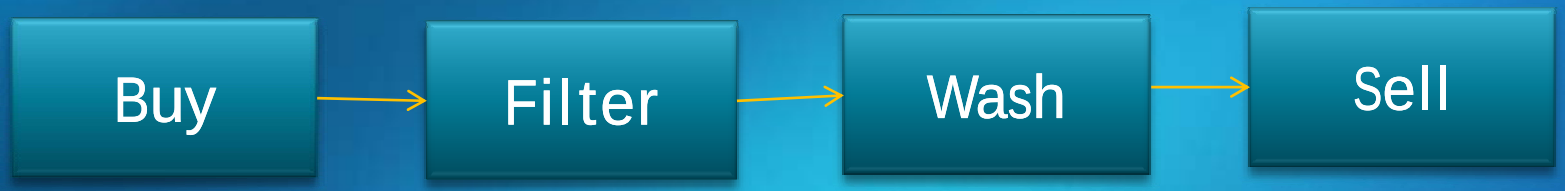
- Login information, a.k.a, username, password and game server address/hostname
- Details of the character, such as level, role and inventory in the game world
- Virtual money collected by the character

Envelopes(contd.)



Envelopes (contd.)

- Wash envelope – change the password of the stolen account, transfer the items away and sell the accounts/items for real money
- Envelopes washers



Stalls

Stalls are the dispatching destinations for stolen envelopes(Email address/Web UI + Database)

Envelop Inbox System for "The Legend of Monkeyking II"- (Customer Support QQ: 26#####0 43######)

Query;: Sort By Time Submit

⏮ 1 ⏭ Page:1/1 Total 74 records 100/Page

ID	Area	Server	Username	Password	Repository Password	Character	Level	Coin	Delete
123	人界	水调歌头	liu********	02**********		刀箭合一	8	0	
Time:2008-4-15 19:30:42 IP:222.***.***.**									
122	推荐	荷塘月色	on*******	be******************		华南天龙	0	0	
Time:2008-4-15 19:19:24 IP:122.**.***.**									
121	人界	水调歌头	za********	lig**********		《神天兵》★	118	270053	
Time:2008-4-15 18:42:57 IP:222.***.***.**									

Stalls (contd.)

Name

Date

Status

Type

In use

Progress

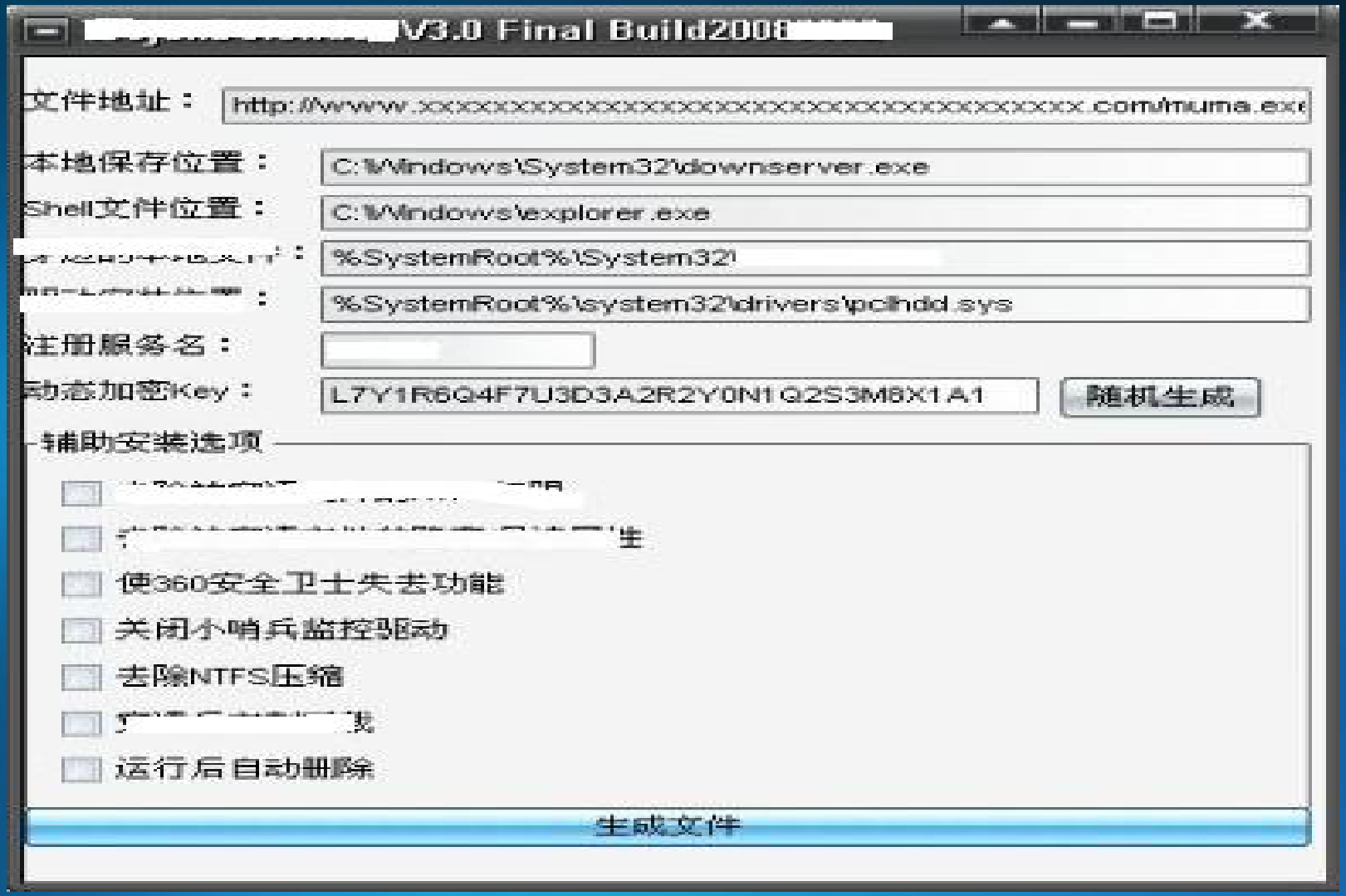
我们一直在努力

箱子时间	箱子名称	进度	今天进度%	日期	服务器状态
月	梦幻西游	收信中	52%	2008-9-21	
月	梦幻西游	收信中	%	2008-9-21	
月	魔兽世界	收信中		008-9-21	
月	征途	信中		008-9-21	
月	大话	信中		008-9-21	
月	魔域	收信中		008-9-21	
月	热血江湖	收信中	98%	2008-9-21	
月	天堂2	收信中	63%	2008-9-21	
月	传奇世界	收信中	28%	2008-9-21	
日	梦幻西游	收信中	100%	2008-9-21	
日	征途世界	收信中	82%	2008-9-21	
月	三国群英传	收信中	67%	2008-9-21	
日	魔域	收信中	90%	2008-9-21	
月	QQ	收信中	95%	2008-9-21	
月	完美世界	收信中	36%	2008-9-21	
月	GF魔兽	收信中	94%	2008-9-21	
日	魔域	收信中	47%	2008-9-21	
日	魔兽世界	收信中	98%	2008-9-21	
日	完美世界	收信中	97%	2008-9-21	

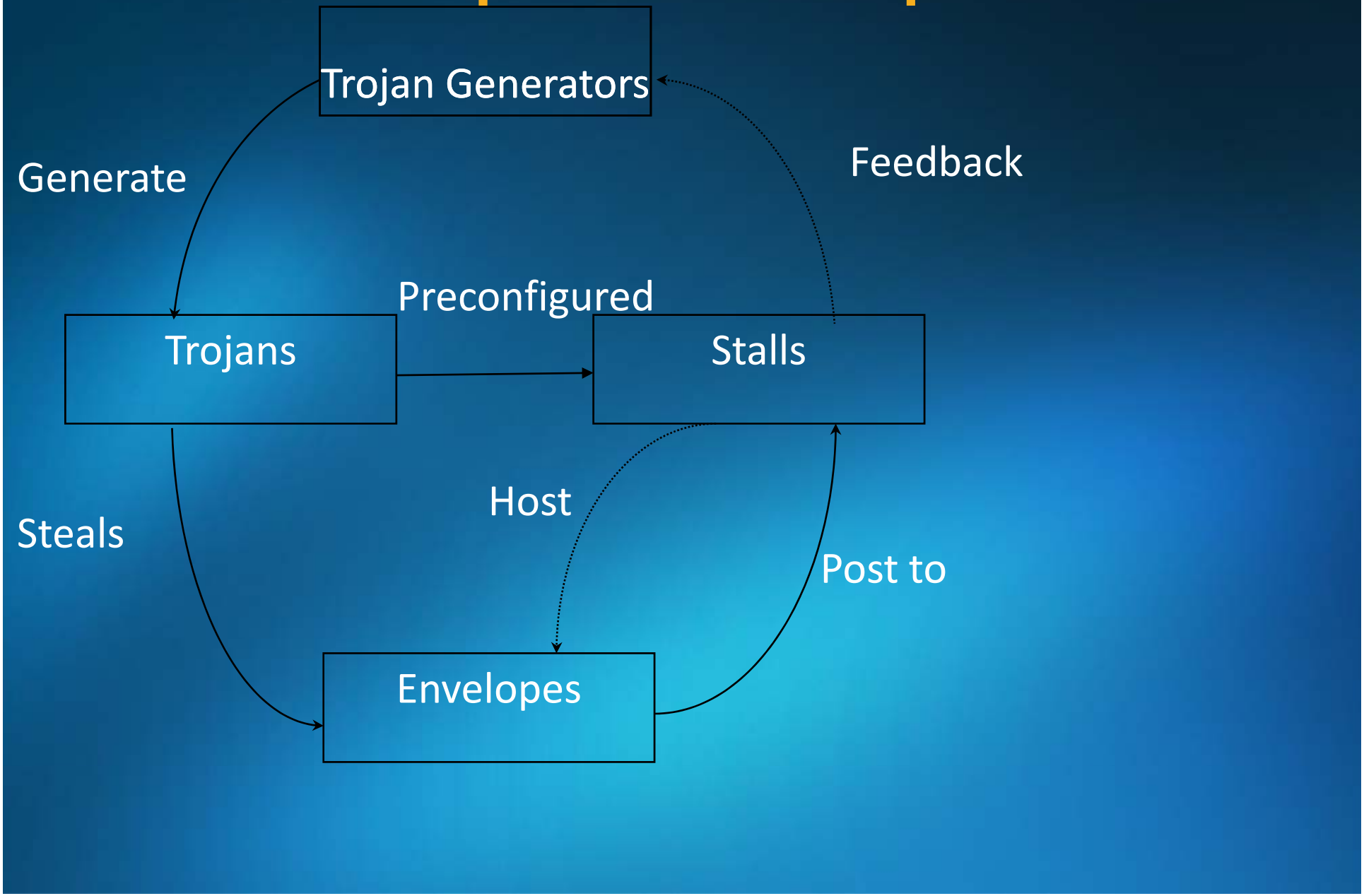
Trojan & Trojan Generators

- Trojan – the malware designed to steal and dispatch envelopes
- Trojan Generators – the tool to generate trojans

Trojan Generators



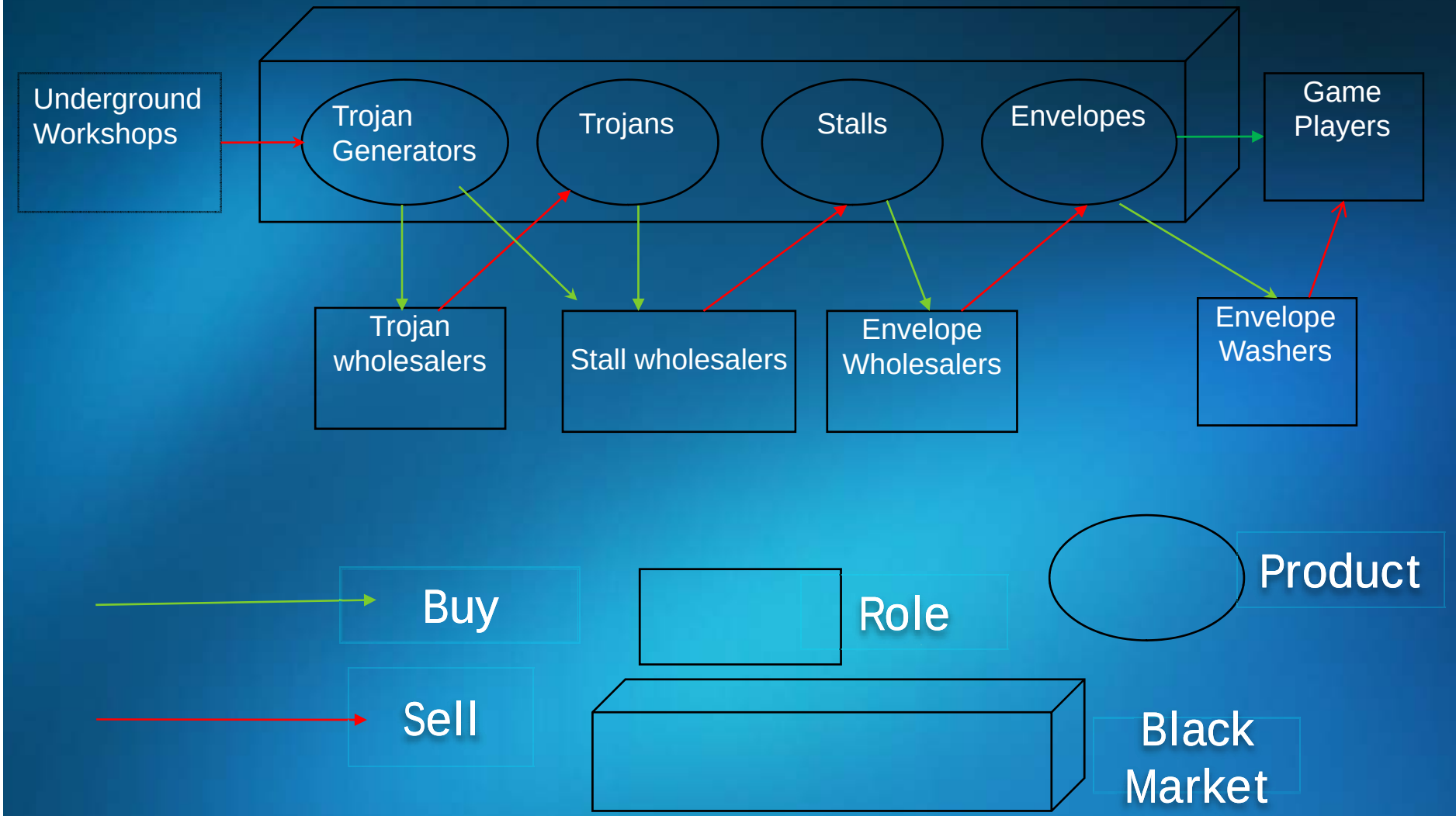
Relationship between products



Which product is for me ?

	Price (USD)	Targeted Buyers	Option Offered by Sellers
Envelopes	Low $1 - $20	End Game Players/Envelope Washers	Sale
Stalls	Very High $100 / month(300 envelopes /day) $40 /day (1800 -2000 envelopes /day)	Game Account wholesalers	Sale or Rent
Trojans	Medium-High $100 (free updates for 3 months)	Stall wholesaler/Game Account wholesaler	Sale and Renew
Trojan Generators	High $300 (free updates for 4 months)	Stall wholesaler/Trojan wholesaler	Sale and Renew

The operation of the black market



Disassembling The Malware

- Malicious software
- Commercial software products

Prevalent game-targeting malware families:

- Frethog
- Taterf
- Dogrobot

Prevalent game-targeting malware families--Frethog

- In the 1st week of MSRT release:
  - 1,374,911 files disinfected
  - 652, 625 distinct machines disinfected

Prevalent game-targeting malware families--Taterf

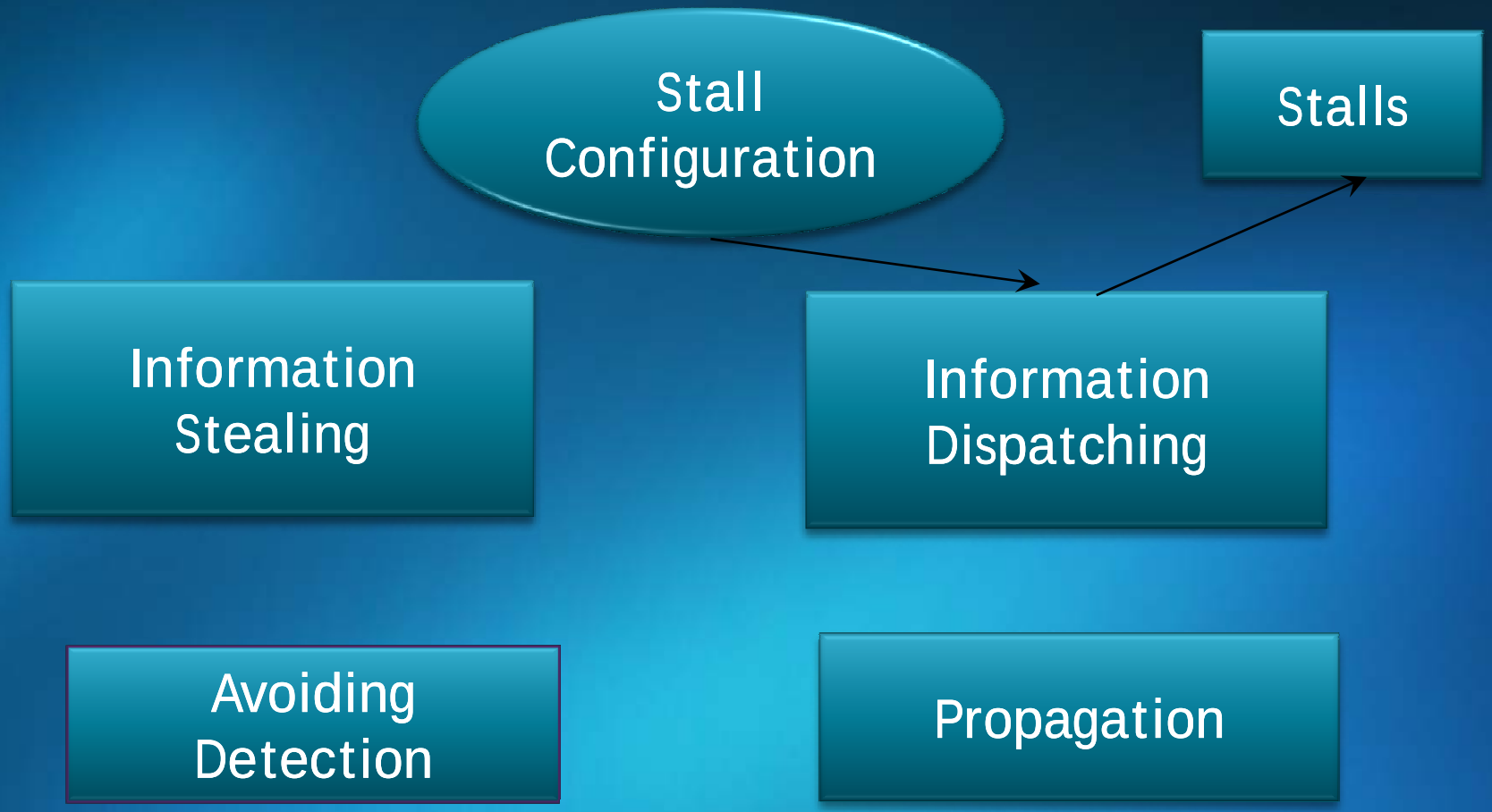
- Taterf = Frethog + removable device /network share drive spread

- In the 1st week of MSRT release:
  - 2,342,399 files disinfected
  - 1,269,098 distinct machines disinfected

Prevalent game-targeting malware families--Dogrobot

- downloader
- bypass system restore hardware (widely used in Internet café)
- Caused more than 1 billion loss to Internet Café in China

Taxonomy of game-targetting malware



Information Stealing Module

- Setup mouse/keyboard hooks
- Read/Write Process memory

Information Dispatching Module/Stall Configuration

- SMTP
- HTTP Post

e.g. http://219.129.239.209/wmgj/lin.asp

Avoiding Detection

- Packers/Encryptors
- Process Termination
- Simulation of user action
- Code obfuscation
- Code Injection
- Anti-Emulation
- Rootkit
- “Companion Virus”(Win32/Junkoil wow.exe ->w0w.exe)

Propagation

- Via other malware

- Via removable device/network share drive (Win32/Taterf)
- Via file infection (Win32/Viking)

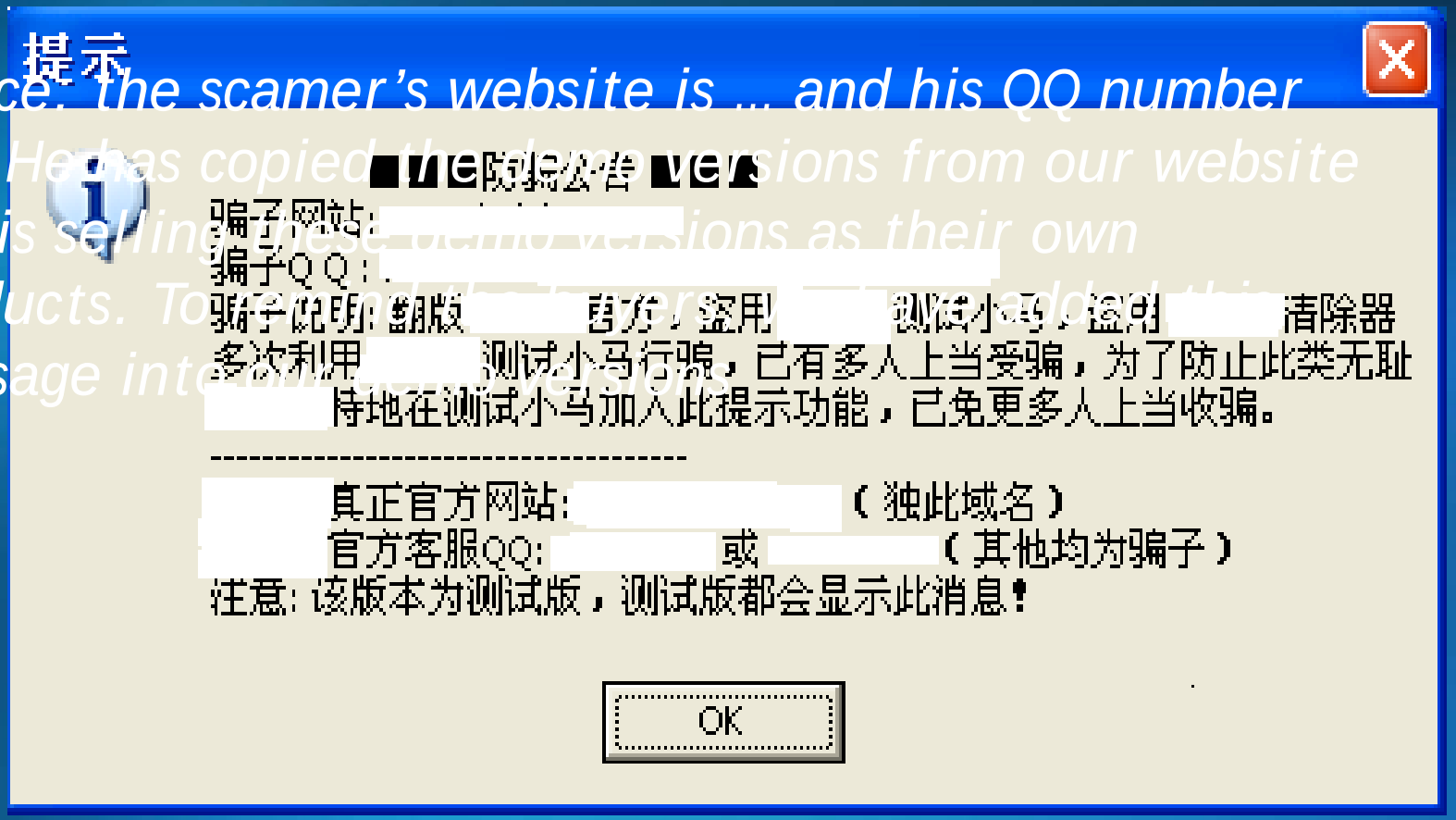
Commercial Software Products Practice

- Sales-websites
- Support-Instant Messaging Tool (QQ)

Commercial Software Products Practice(Contd)

Competition (Buy from us!)

Notice: the scamer's website is ... and his QQ number is.... He has copied the demo versions from our website and is selling these demo versions as their own products. To combat this we have added this message into our software.



Practise commercial Software Products(Contd.)

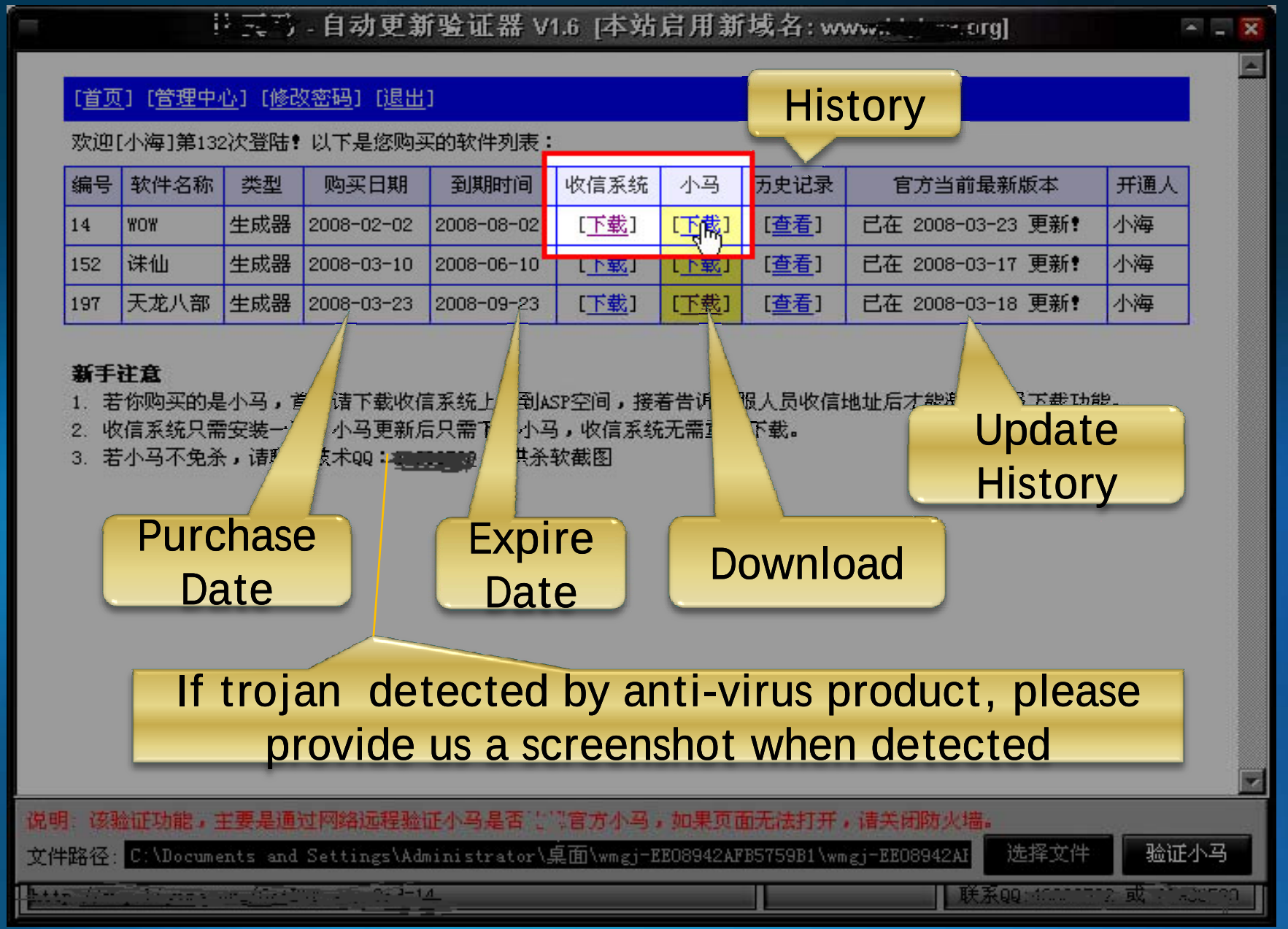
Product Testing

- Quality Assurance
- Survival Test

Commercial Software Products Practice (contd.)

Maintenance/Upgrade to avoid detection

- Auto update
- Manual update


自动更新验证器 V1.6 [本站启用新域名:www.[redacted].org]
[首页] [管理中心] [修改密码] [退出]
欢迎[小海]第132次登陆！以下是您购买的软件列表：
编号 软件名称 类型 购买日期 到期时间 收信系统 小马 历史记录 官方当前最新版本 开通人
14 WOW 生成器 2008-02-02 2008-08-02 [下载] [下载] [查看] 已在 2008-03-23 更新！ 小海
152 诛仙 生成器 2008-03-10 2008-06-10 [下载] [下载] [查看] 已在 2008-03-17 更新！ 小海
197 天龙八部 生成器 2008-03-23 2008-09-23 [下载] [下载] [查看] 已在 2008-03-18 更新！ 小海
新手注意
1. 若你购买的是小马，首[redacted]请下载收信系统上[redacted]到ASP空间，接着告诉[redacted]服人员收信地址后才能[redacted]下载功能。
2. 收信系统只需安装一[redacted]小马更新后只需下[redacted]小马，收信系统无需重[redacted]下载。
3. 若小马不免杀，请[redacted]技术QQ：[redacted]杀软截图
History
Update History
Purchase Date
Expire Date
Download
If trojan detected by anti-virus product, please provide us a screenshot when detected
说明：该验证功能，主要是通过网络远程验证小马是否[redacted]官方小马，如果页面无法打开，请关闭防火墙。
文件路径：C:\Documents and Settings\Administrator\桌面\wmgj-EE08942AFB5759B1\wmgj-EE08942AF
选择文件
验证小马
联系QQ[redacted]或[redacted]

Conclusion

The black market poses comprehensive challenge for:

- Game Players
- Antivirus vendors
- Game Vendors
- Other Business
- Law makers

Microsoft®

Your potential. Our passion.™

© 2008 Microsoft Corporation. All rights reserved. Microsoft, Windows, Windows Vista and other product names are or may be registered trademarks and/or trademarks in the U.S. and/or other countries.
The information herein is for informational purposes only and represents the current view of Microsoft Corporation as of the date of this presentation. Because Microsoft must respond to changing market conditions,
it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information provided after the date of this presentation.
MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS PRESENTATION.

Questions & Answers

Questions et réponses