Microsoft®

tech·ed

中国 | 2010

1-3 December 2010 | Beijing, China

SIA-200-1

Microsoft® tech·ed 中国 | 2010

1-3 December 2010 | Beijing, China

网络威胁形势与终端安全

吴志雄 (Scott Wu)
项目经理 (Program Manager)

主要内容

- 全球安全报告
- 中国网络威胁形势
- 网络地下经济案例分析
- 终端安全：Forefront技术及测试认证
- 终端安全：Forefront及企业安全
- 总结

全球安全报告
与中国网络威胁形势

全球安全报告

微软 TwC 安全

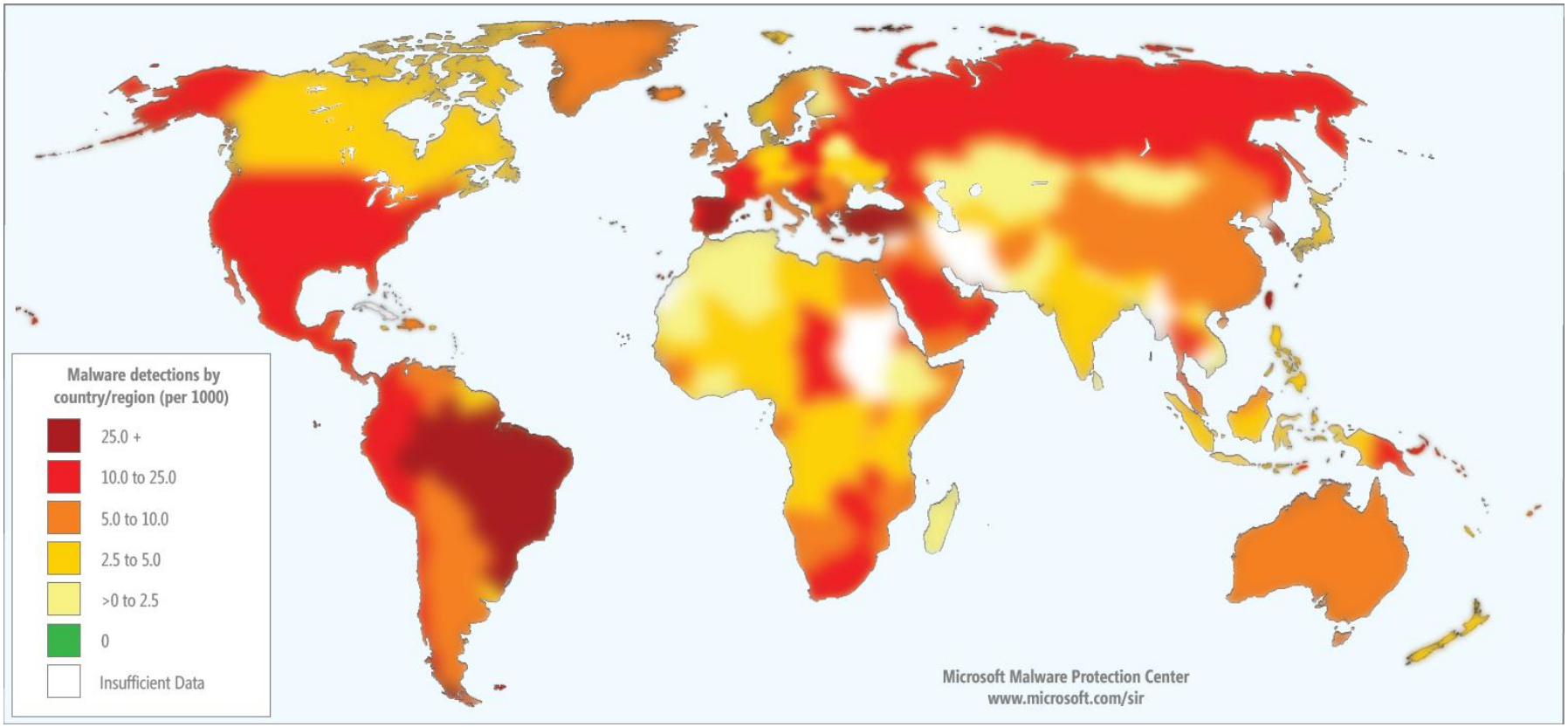
从整体保护客户及软件行业研发应用到维护生态环境

Microsoft Malware Protection Center (MMPC)

Microsoft Security Engineering Center (MSEC)

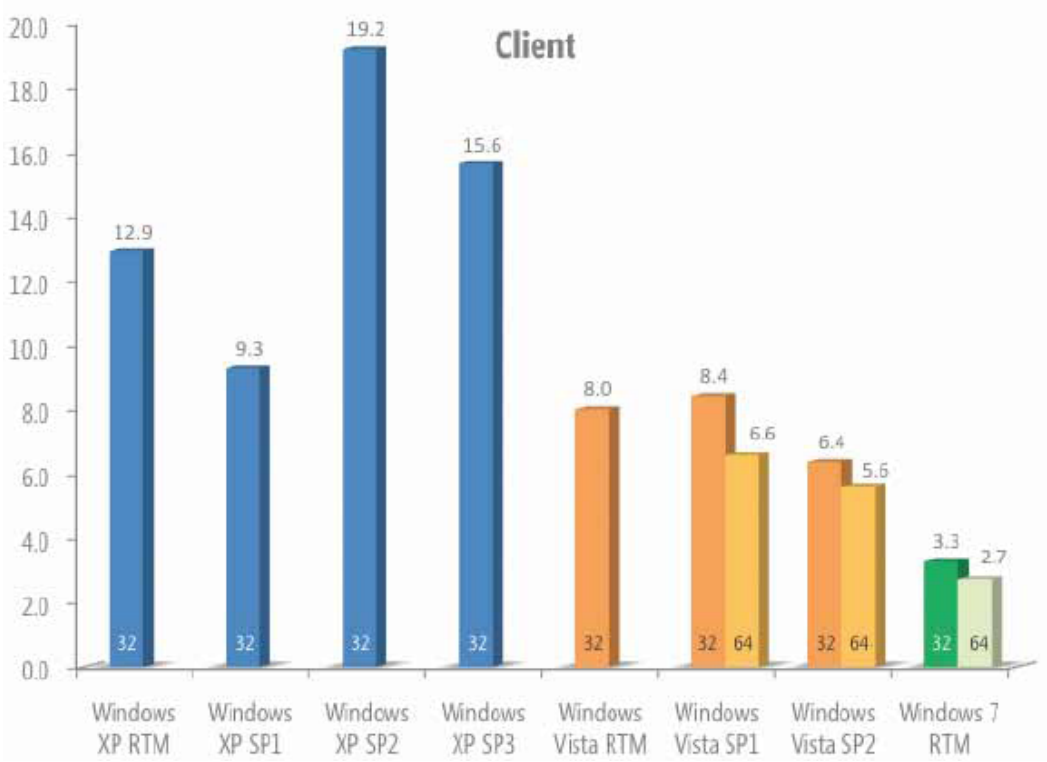
Microsoft Security Response Center (MSRC)

全球恶意软件以及可疑软件

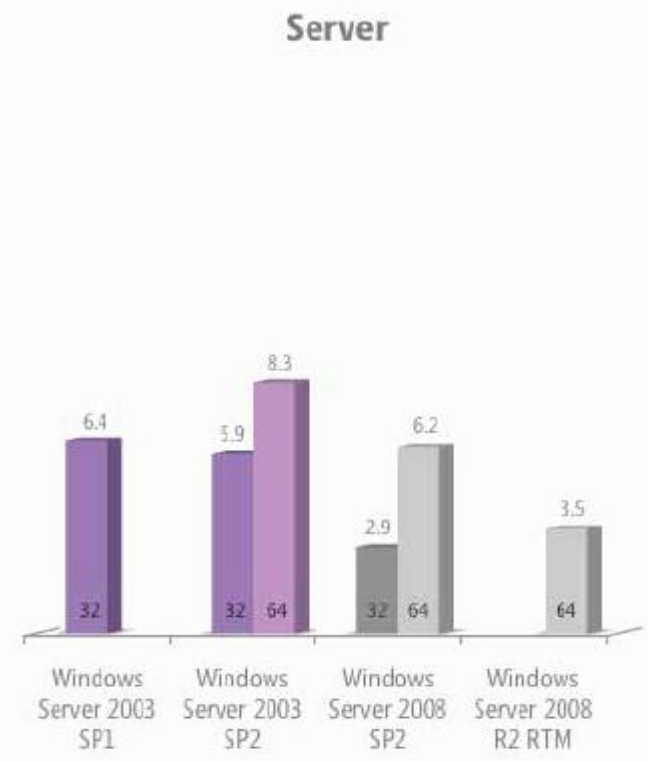


恶意软件以及可疑软件
操作系统分布

终端



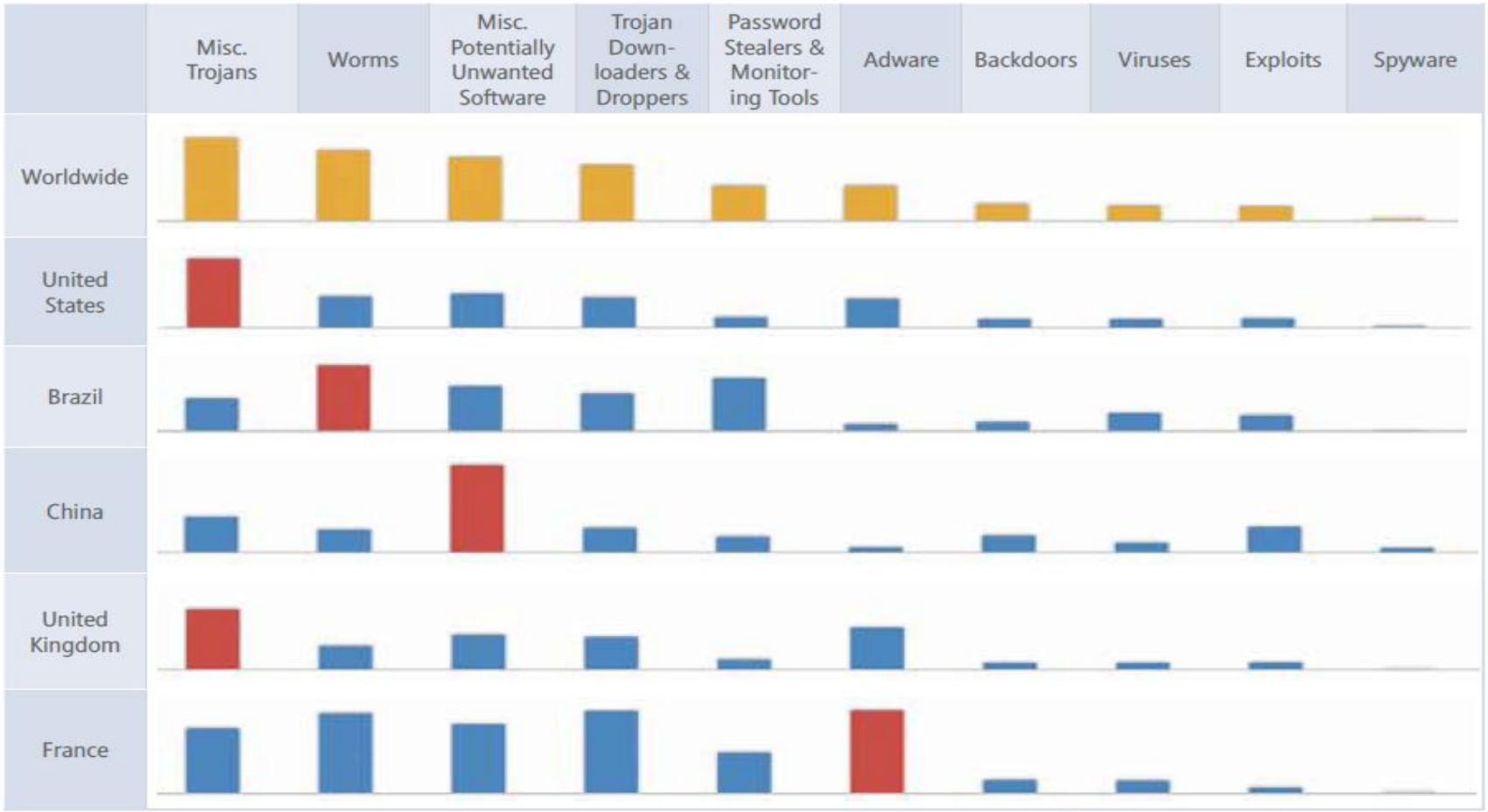
服务器



2010第二季度，每运行1000次MSRT所清理的电脑数量

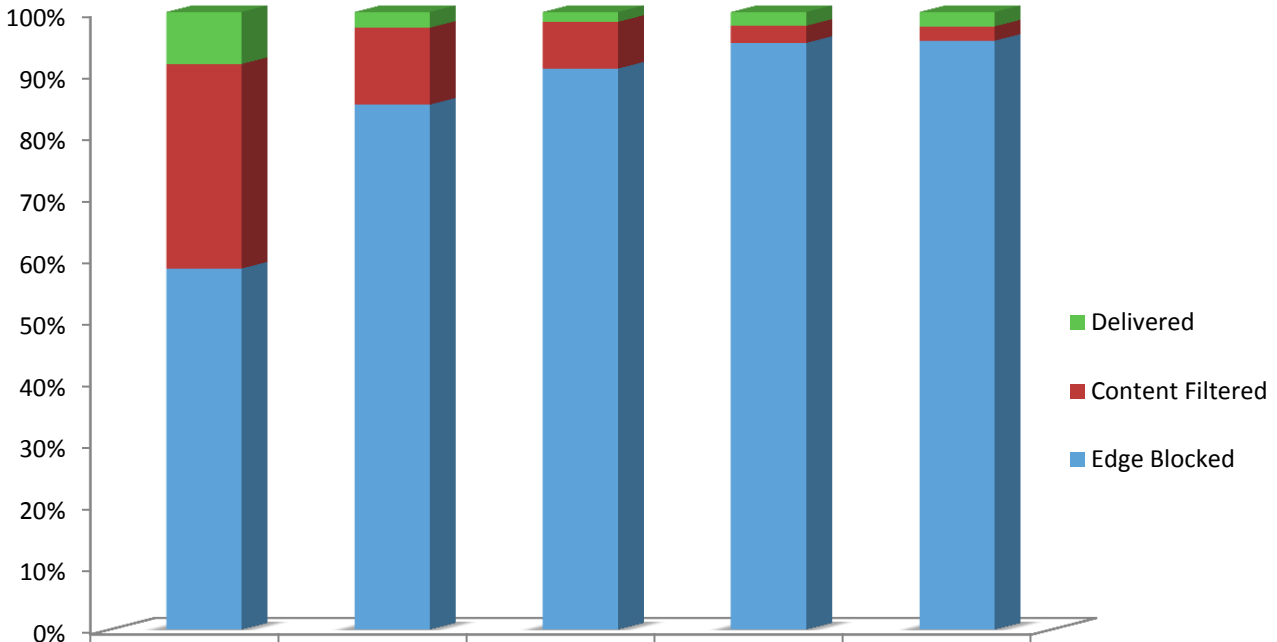
网络安全地域区别

不同地域的情况有所差异



垃圾邮件趋势

2010 第二季度， Forefront Online Protection for Exchange (FOPE)



	2006	2007	2008	2009	2010
Delivered	9,740,907,973	11,594,625,114	16,944,213,823	17,383,913,329	10,811,833,125
Content Filtered	38,258,227,962	56,616,565,058	79,798,550,868	21,511,330,566	10,763,446,377
Edge Blocked	67,655,543,019	386,982,872,08	959,428,000,00	738,676,583,40	442,572,855,07

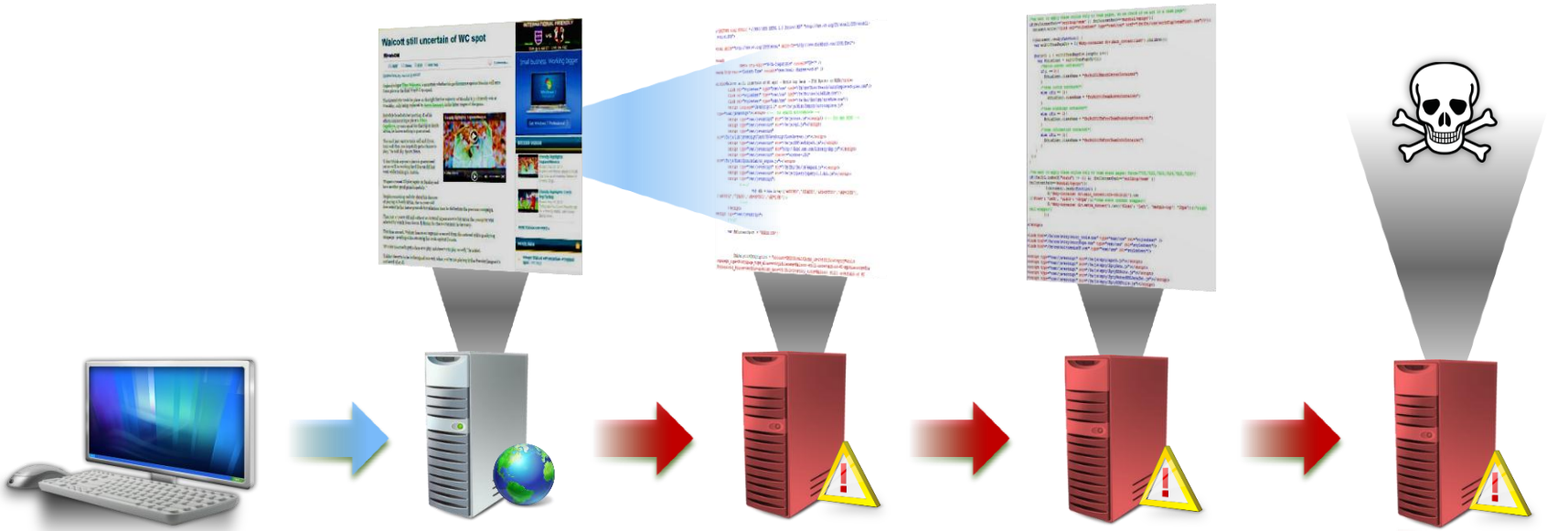
偷渡式下载攻击（Drive-by）

从有漏洞电脑
访问被挂网页
（比如有隐藏 Iframe）

隐藏IFrame
秘密载入另一网页

转向藏有漏洞利用的网页

漏洞利用成功
下载恶意软件到终端用户



用户

恶意或被挂马的网站

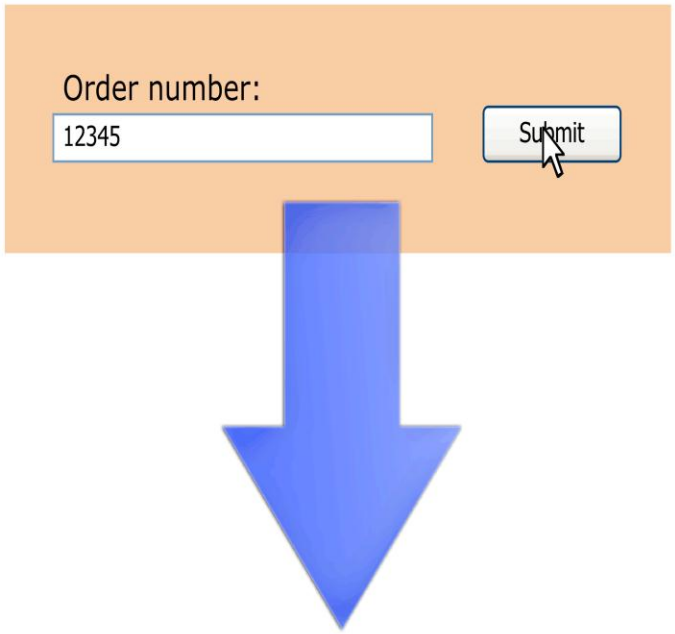
转向器
(Redirector)

漏洞利用服务器
（Exploit Server）

恶意软件服务器
（Malware Server）

自动SQL注入攻击(SQL Injection)

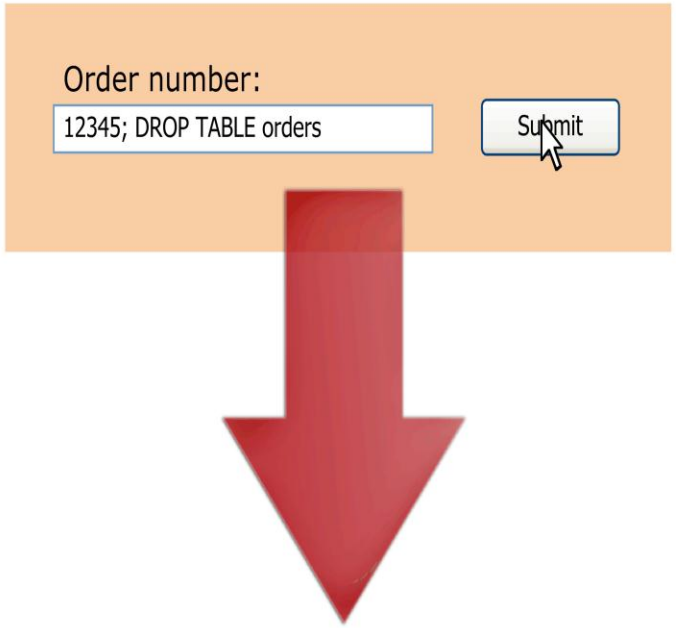
Text entered in a Web form is used to construct a SQL query to add or retrieve information from a database.




```
SELECT * FROM orders WHERE OrderID = 12345;
```

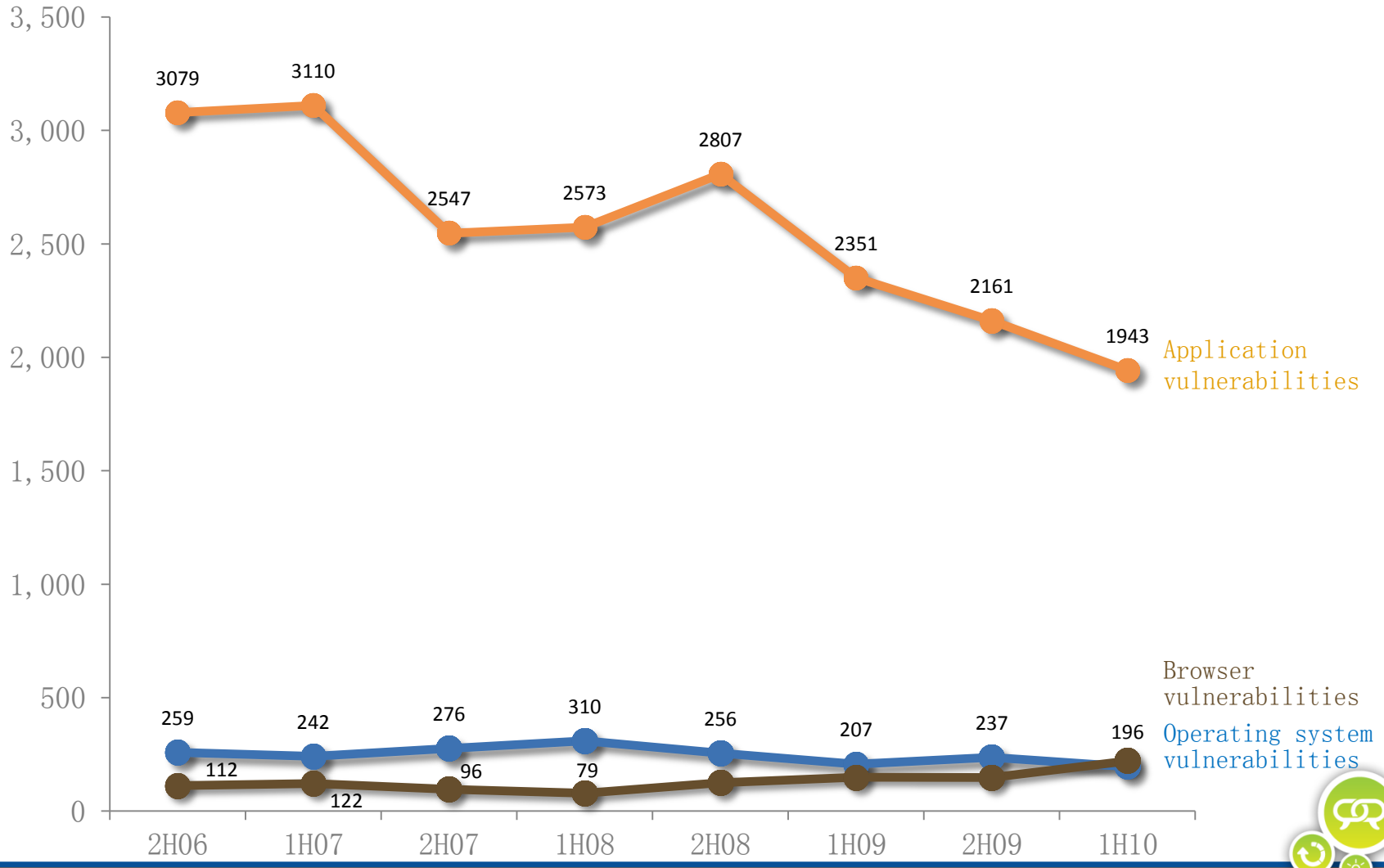
Microsoft Malware Protection Center
http://www.microsoft.com/security/portal

If the text entered is not properly validated, an attacker can use it to execute arbitrary SQL statements that perform damaging actions, such as deleting tables.

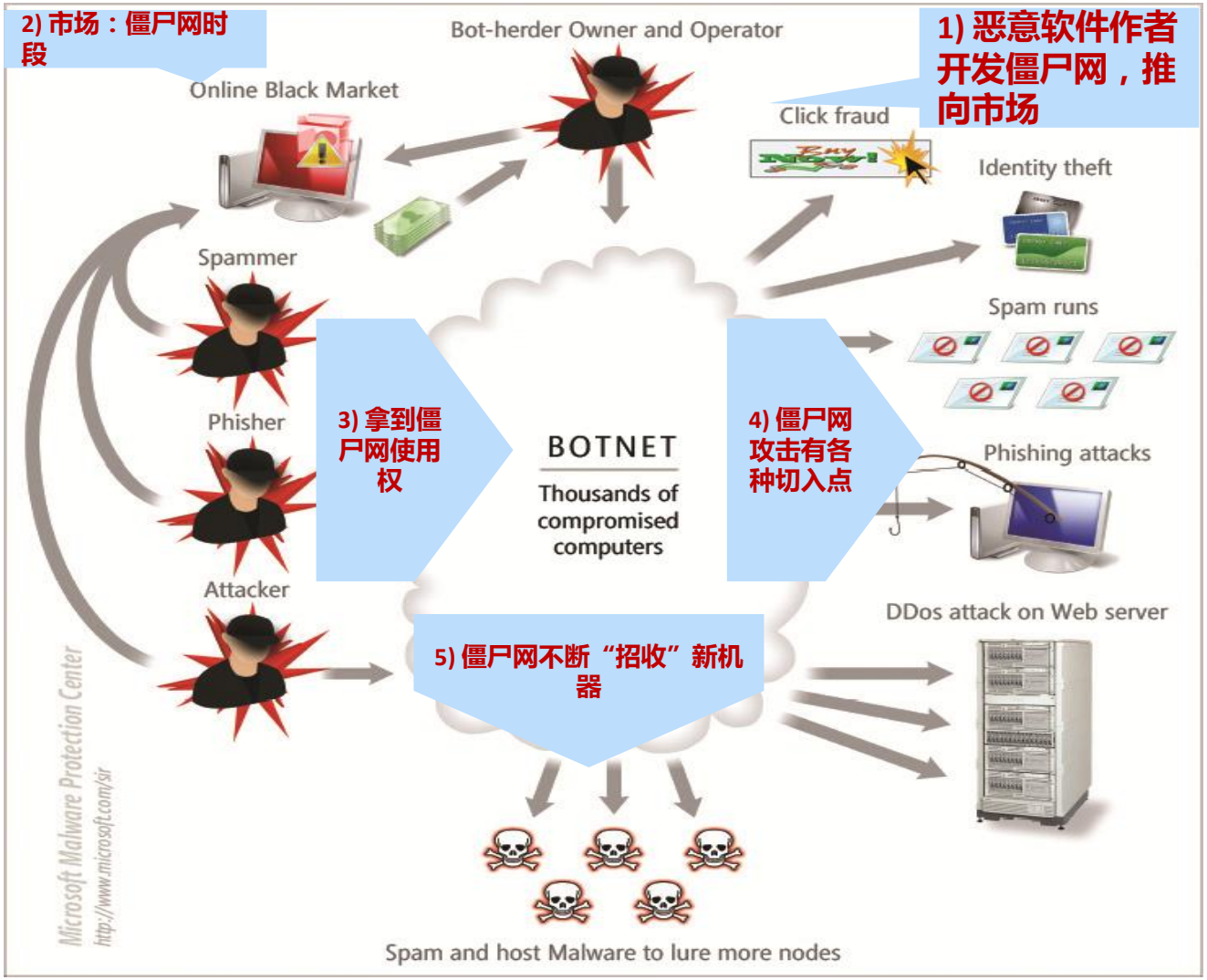



```
SELECT * FROM orders WHERE OrderID =
12345; DROP TABLE orders;
```

漏洞披露
操作系统，浏览器及第三方软件

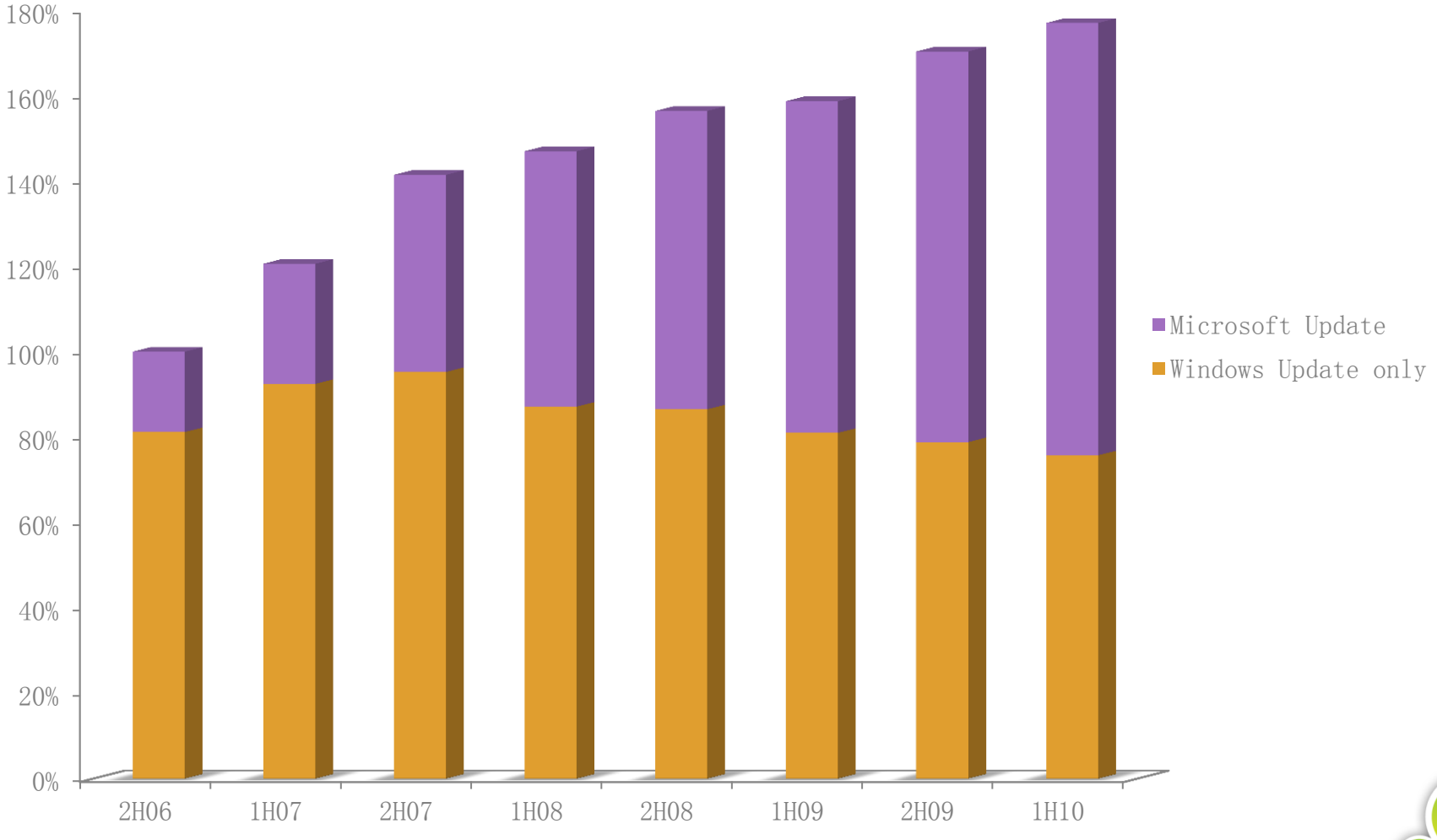


僵尸网络(botnet)


2) 市场：僵尸网时段
Bot-herder Owner and Operator
1) 恶意软件作者开发僵尸网，推向市场
Online Black Market
Click fraud
Identity theft
Spammer
Spam runs
Phisher
3) 拿到僵尸网使用权
BOTNET
Thousands of compromised computers
4) 僵尸网攻击有各种切入点
Phishing attacks
Attacker
DDos attack on Web server
5) 僵尸网不断“招收”新机器
Microsoft Malware Protection Center
http://www.microsoft.com/sir
Spam and host Malware to lure more nodes

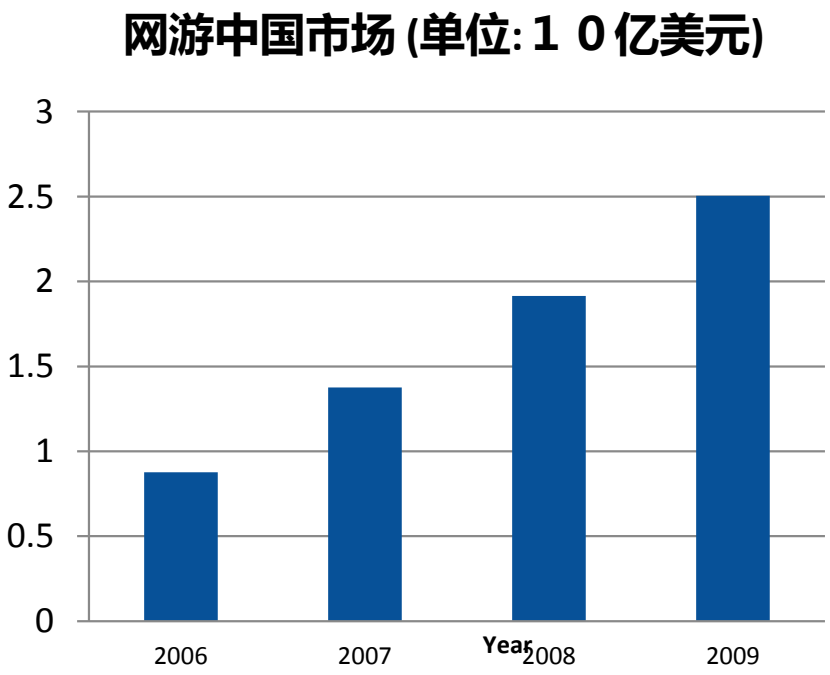
更新服务

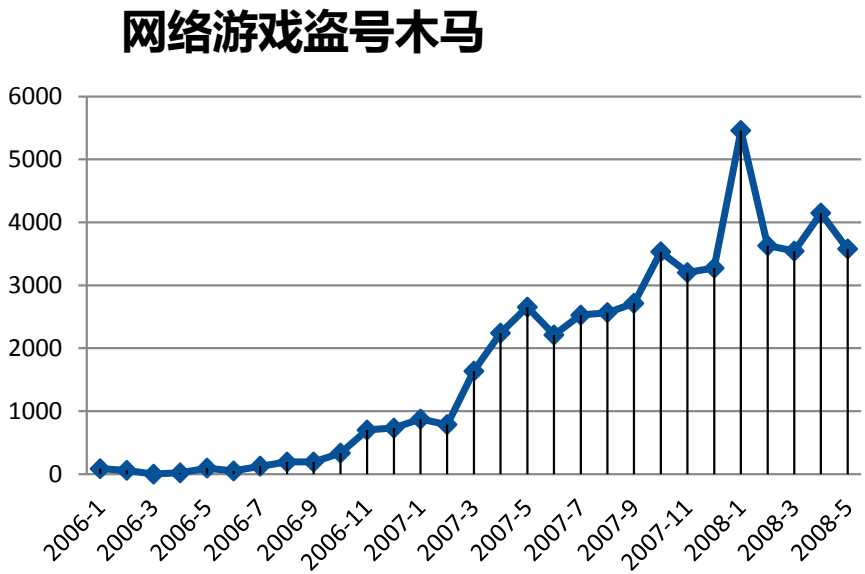
Windows Update (WU) 及Microsoft



网络地下经济案例分析

中国网络地下经济 – 案例分析
网络游戏盗号木马





写木马，开宝马

网络游戏市场

- 魔兽世界 (WoW)用户
  12，000，000
  (2010年)
- 中国网游用户
  217，000，000
  (2010年)

- 级别： 时间=金钱
  WOW L70 = 360 hours
- 虚拟物品
  稀货 = $1500
- 虚拟货币
  1000魔兽金币 = $30







网络游戏盗号木马的演变

- 针对国内网吧

2007年9月

机器狗
Win32/Dogrobot

首例针对还原卡的盗号木马

2008年6月

Win32/Dexfom

寄生感染盗号病毒

2009年12月

Win32/Checkafe

针对主机/账号绑定的木马

2010年3月

WinNT/Ghodow

感染主引导记录MBR

网络游戏盗号木马市场

木马市场

- 产品
- 买家
- 卖家

产品

- 信封 ($1-$20)
- 箱子 ($100+/month)
- 木马 ($100)
- 木马生成器 ($300)

演示：破解矩阵卡

	1	2	3	4	5	6	7	8
A	03	25	96	06	38	68	44	57
B	58	08	46	91	40	52	05	63
C	76	88	55	09	30	87	85	27
D	19	09	84	11	22	76	17	30
E	28	83	69	34	22	99	33	19
F	33	71	21	66	04	41	05	55
G	64	83	47	76	12	62	14	08
H	39	04	62	78	60	83	28	48
I	87	77	05	48	01	36	88	29
J	95	16	22	95	46	21	42	36

网络游戏盗号木马的启示

- 确保系统及时更新 (微软及第三方软件)
- 开启Windows Update （ WU)
- 安装可靠防毒软件
- 安装防火墙
- 不要共享密码
- 使用强密码

但是---如何实现企业安全自动化？

终端安全

保护客户端和服务器计算机操作系统不受日益严峻的病毒威胁、防止数据丢失并实现几乎可从任何地方进行安全地访问

随地**保护**
随处**访问**

- 防御针对终端的复杂威胁
- 保护敏感信息
- 提供更加安全和随时可用的访问

整合并**扩展**安全

- 结合操作系统安全
- 优化现有基础架构

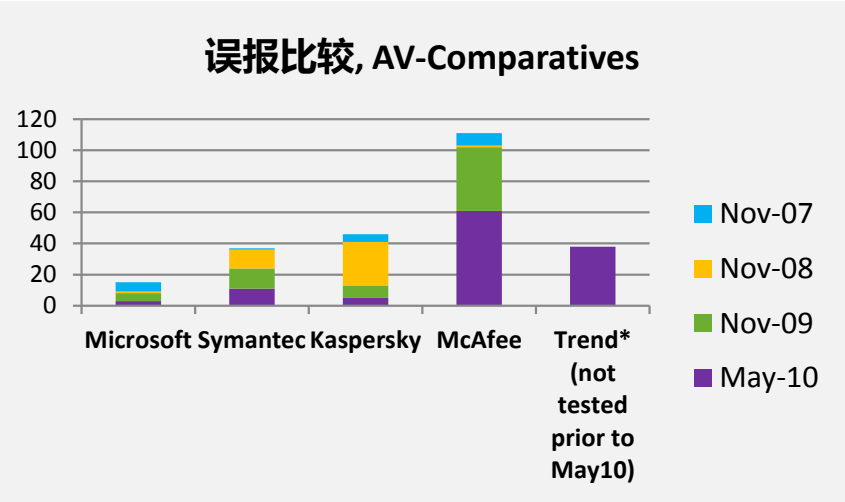
简化安全
管理一致性

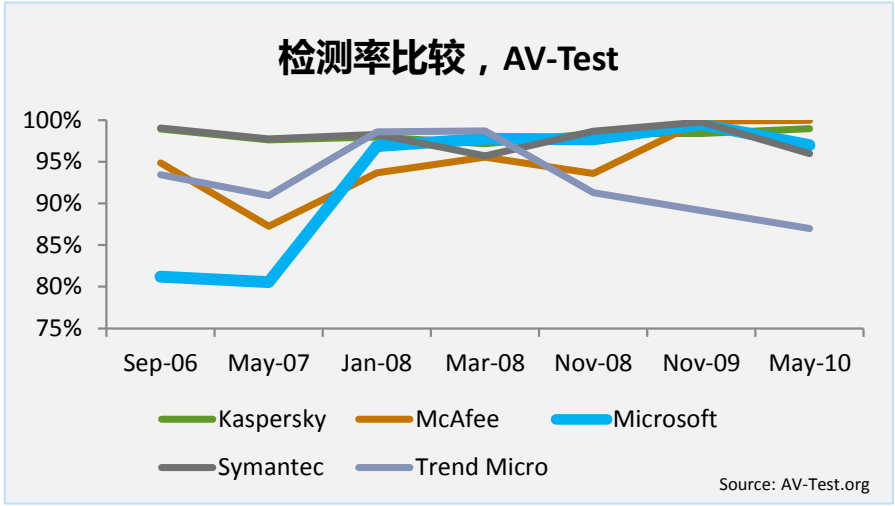
- 使用统一的管理控制台简化管理
- 洞悉整个企业的安全状态

终端安全

Forefront技术及测试认证

Forefront Endpoint Protection
过硬的测试与认证指标





综合比较，AV-Comparatives.org

	On-Demand	Pro-active	Performance	Dynamic	Removal	PUA
Microsoft	**Advanced**	Advanced+	Advanced+	Advanced	Advanced+	Advanced
Symantec	Advanced+	Advanced	Advanced+	Advanced+	Advanced+	Advanced+
McAfee	Advanced	Standard	Advanced+	Standard	Advanced	Advanced+
Kaspersky	Advanced	Advanced+	Advanced+	Advanced+	Advanced+	Advanced
Trend Micro	Tested	Standard	Withdrew	Withdrew	Withdrew	Withdrew

主要安全检测机构

- 认证检测
  - ICSA (Verizon Business)
  - West Coast Labs Checkmark (Haymarket Media)
  - Common Criteria
  - 中国公安部计算机病毒防治产品检验中心
- 评比检测
  - AV-Test.org
  - AV-Comparatives.org
  - Virus Bulletin (VB)
  - PC 安全实验室（PCSL/中国)
- 浏览器检测
  - NSS Labs

认证模块（ICSA / West Coast Labs）

- 认证检测的模块
  - 恶意软件检测
  - 恶意软件清除
  - 流氓软件（此模块渐失价值）
- 质量门槛
  - 100% of WildList
  - 95-97%恶意软件库检测率
  - 无误报
  - 清除成功

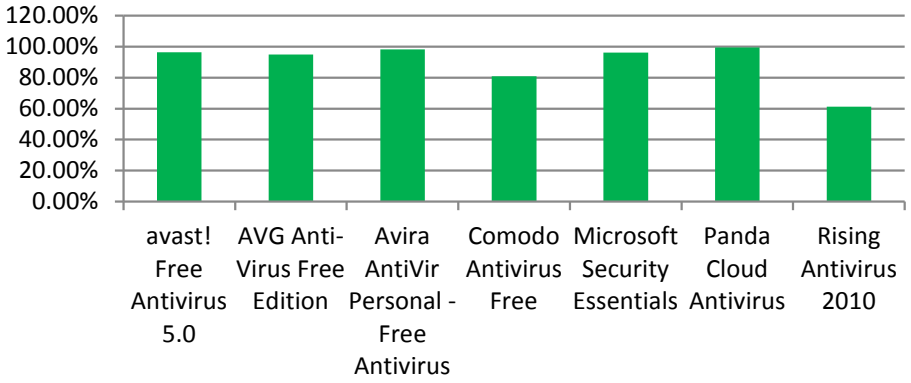
杀毒认证覆盖面

- 连续通过每月认证测试

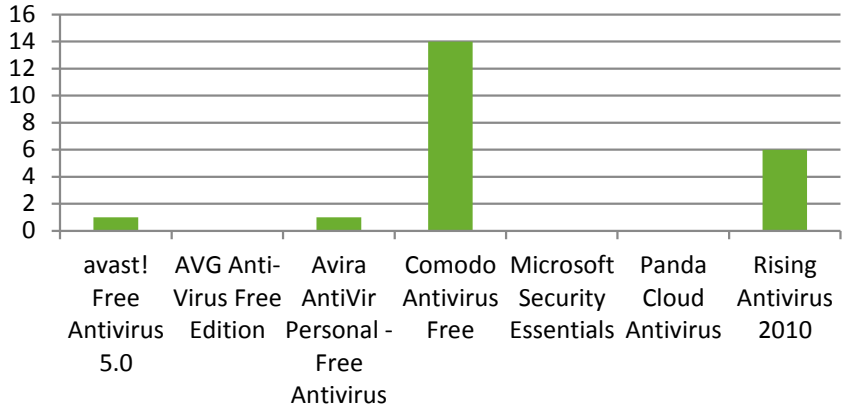
		West Coast Labs认证								ICSA认证					
		AV 检测		AV 清除		Anti-trojan		Anti-spyware		AV 检测		AV 清除		Anti-spyware	
		x86	x64	x86	x64	x86	x64	x86	x64	x86	x64	x86	x64	x86	x64
MSE	XP	X		X		X		X		X		X			
	Vista	X		X		X		X		X		X			
	Win 7		X		X		X	X		X	X	X	X		
FCS	XP	X		X		X									
	Vista	X		X		X				X	X	X	X		X
	Win 7							X			X		X		
	Server08		X		X		X		X				X		X

AV-Test.org
德国c't 杂志2010五月测试

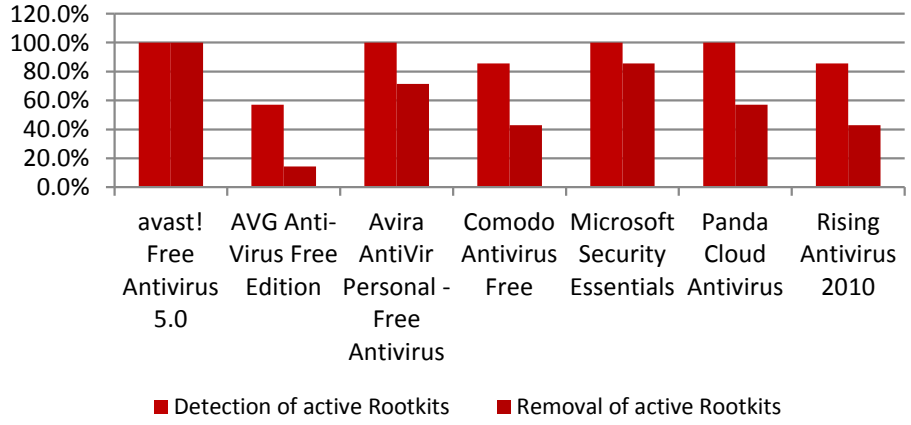
检测率 (恶意软件库)



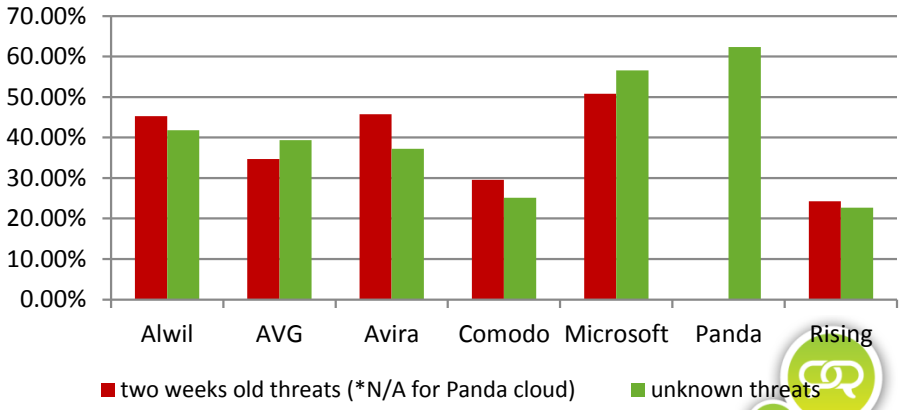
误报



Rootkit Testing



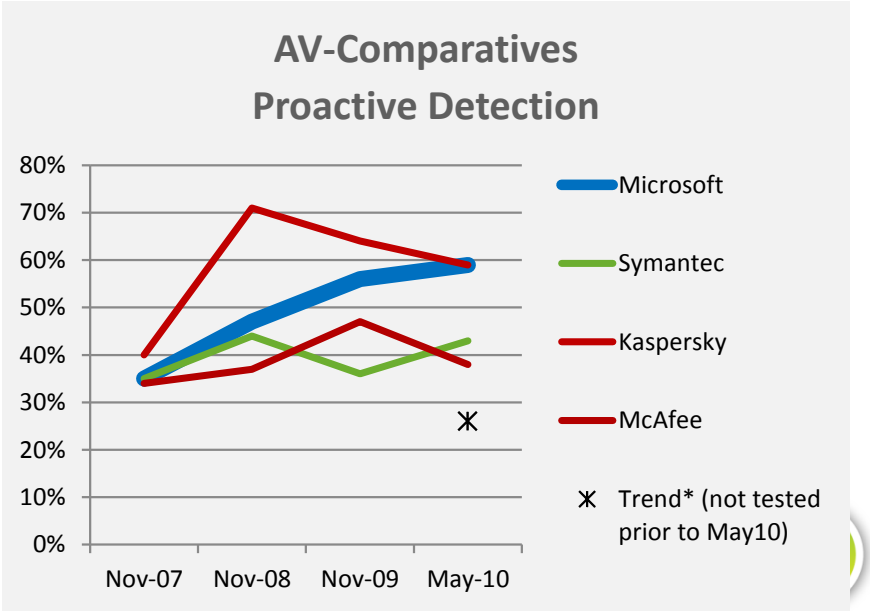
未知和最新恶意软件



AV-Comparatives.org
前摄性检测（未知病毒）

- 新病毒检测有效率
- 方法
  - 冻结杀毒软件及病毒定义
  - 继续收集恶意软件样本

Proactive Detection Testing	
Test Date	**Award Level**
May-10	**Advanced+**
Nov-09	Advanced+
May-09	Advanced+
Nov-08	Advanced
May-08	Advanced
Nov-07	Advanced
May-07	Standard



AV-Comparatives.org
静态测试(2010八月)

主要杀毒公司	评比级别	检测率	误报
Symantec	Advanced+	98.7%	9
Microsoft	**Advanced***	**97.6%**	3
Sophos	Advanced	96.8%	13
McAfee	Advanced	99.4%	24
Kaspersky	Advanced	98.3%	46
Trend Micro	Tested	90.3%	23

	Detection Rate			
	< 90%	90 - 95%	95 - 98%	98 - 100%
Few (0-15 FP's)	TESTED	STANDARD	ADVANCED	ADVANCED+
Many (16-100 FP's)	TESTED	TESTED	STANDARD	ADVANCED
Very many (101-500 FP's)	TESTED	TESTED	STANDARD	STANDARD
Crazy many (over 500 FP's)	TESTED	TESTED	TESTED	TESTED

* *若按原来评定方法微软该得Advanced+*

AV-Comparatives

2010二月：云cloud vs. 非云no cloud

Vendor	On-Demand	False Alarms	Rating
Trend Micro (no cloud)	68.5%	22	*Would have been "Tested"*
Trend Micro (with cloud)	90.7%	38	Tested
Panda (no cloud)	73.3%	32	*Would have been "Tested"*
Panda (with could)	98.9%	47	Adv
McAfee (no cloud)	94.9%	19	*Would have been "Standard"*
McAfee (with could)	98.9%	61	Adv

	Detection Rates			
	<87%	87 - 93%	93 - 97%	97 - 100%
Few (0-15 FP's)	TESTED	STANDARD	ADVANCED	ADVANCED+
Many (over 15 FP's)	TESTED	TESTED	STANDARD	ADVANCED

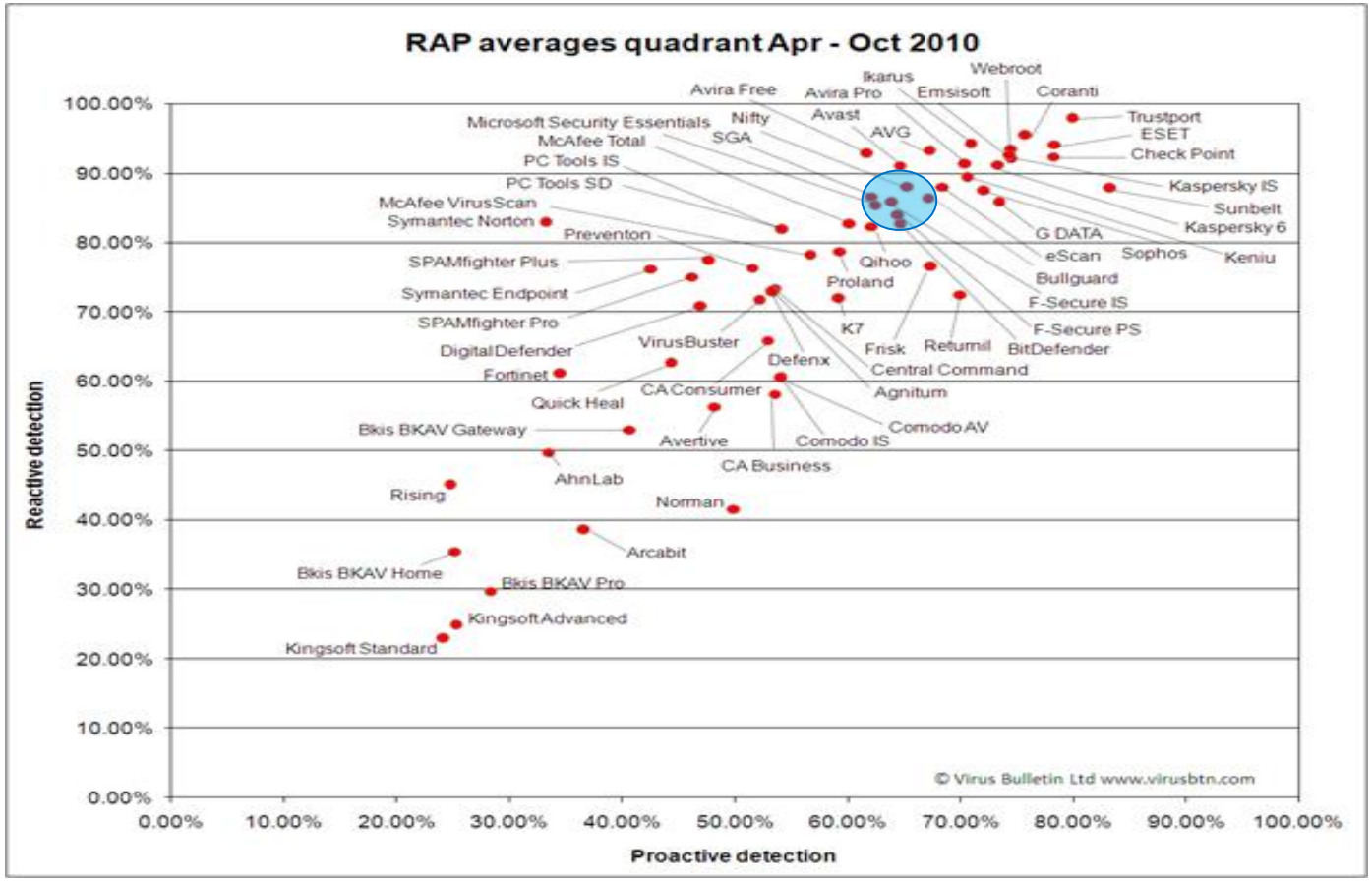
Virus Bulletin (VB)

- VB100
  - 100% WildList
  - no FPs
  - 每两月一测
  - 3次桌面，2次服务器，1次 Linux
- Microsoft
  - 最近19次内通过18次

- **谁 / 何时没通过**
  - Symantec: 08/2009
  - McAfee: 02/2009, 04/2008, 02/2007
  - Trend Micro: 04/2008, 连续 3 次 [后退出]
  - Kaspersky: 04/2010, 10/2008, 06/2008, 12/2007
  - Sophos: 10/2009, 04/2008, 12/2007
  - CA: 12/2010, 12/2009, 10/2008,08/2008
  - Microsoft: 04/2010

VB100 RAP 比较

- 最近3周恶意软件样本
- 未来一周新/未知恶意软件样本



PC安全实验室（PCSL)

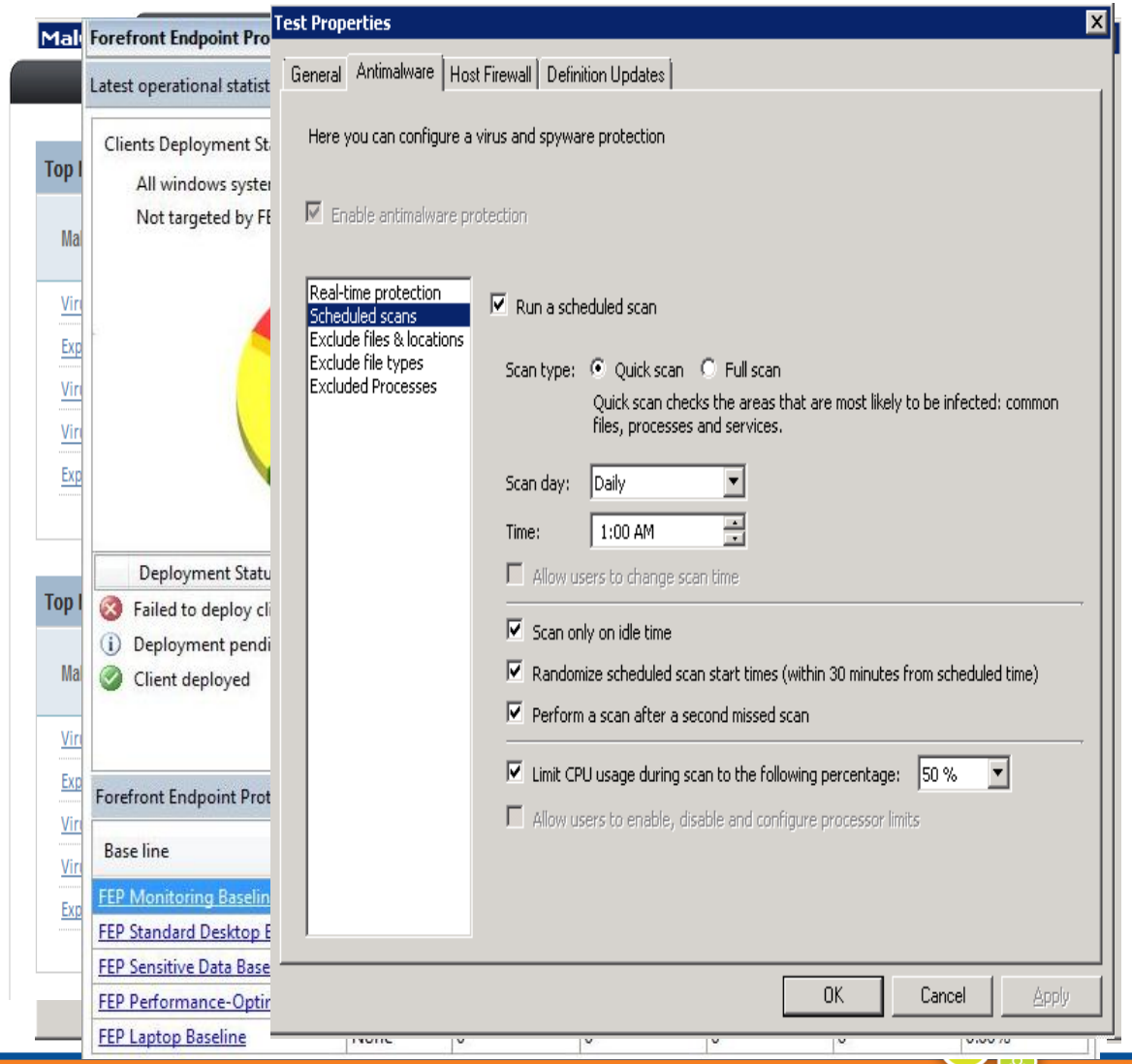
高质量检测

- 必须考虑误报因素
  - Forefront 全力预防误报
  - 杀毒引擎 供给6亿用户
- 必须考虑遥测数据
  - 多样本不代表测试更好更全面
  - 病毒样本是否对用户有影响？

终端安全
Forefront及企业安全

简易安全政策管理

- 样板定义
- “颗粒化”定制
- 软件式发行安全政策
- 终端超级简易化
- 单一管理控制板
- 完整的戒备系统
- 报表及跟踪
- 恶意软件活跃状态



演示： FEP 2010

总结

- 了解国内外网络威胁形势
- 认识Forefront强有力技术指标
- 将安全Forefront终端自动保护

Microsoft®
tech·ed
中国|2010

2010 12.01-03 | 中国 ,北京

疑问和解答

感谢您参与此会场！

您的意见与建议对我们非常重要。

请您填写反馈表。

Microsoft®

您的潜力，我们的动力

欢迎加入微软技术社区 China Technical Audience Community

http://www.microsoft.com/china/community

技术驱动，创建未来

您将获得**最新的微软技术**

您将结识**IT界志同道合的朋友**

您将得到**职业生涯更好的发展机会**

以博会友—立即参与"博客无双"活动

http://zt.cnblogs.com/blogswarriors/

- 写博客，赚积分，赢大礼
- 分享您的TechED参会心得
- 业内权威专家点评推荐

我们倾听您的声音～立即登入微软技术论坛！

http://social.msdn.microsoft.com/forums/zh-CN/

- 与TechEd 2010的讲师群作最直接的沟通
- 与MVP、微软技术社区精英进行交流
- 解答您的技术疑惑，倾听您的宝贵建议