Microsoft Security Intelligence Report Volume 8

Some notes about the presenter…

Feliciano Intini

Responsabile dei programmi di Sicurezza e Privacy di Microsoft Italia

- NonSoloSecurity Blog: http://blogs.technet.com/feliciano_intini
- Twitter: http://twitter.com/felicianointini

Four Areas to Discuss Today

1. Introduction - Microsoft Security Intelligence Report (SIR)
2. Today's Threats - SIR v.8 New Findings – Italy view
3. Advancements in Software Protection and Development
4. What the Users and Industry Can Do

Introduction Microsoft Security Intelligence Report (SIR)

About Security Intelligence Report volume 8

- The 8th volume of the Security Intelligence Report contains data and intelligence from the past several years, but focuses on the second half of 2009 (2H09)
- Full document covers
  - Malicious Software & Potentially Unwanted Software
  - Email, Spam & Phishing Threats
  - Focus sections on:
    - Malware and signed code
    - Threat combinations
    - Malicious Web sites
  - Software Vulnerability Exploits
    - Browser-based exploits
    - Office document exploits
    - Drive-by download attacks
  - Security and privacy breaches
  - Software Vulnerability Disclosures
    - Microsoft Security Bulletins
    - Exploitability Index
    - Usage trends for Windows Update and Microsoft Update

SIR v8: Three Points of View

- Microsoft Malware Protection Center (MMPC)
- Microsoft Security Response Center (MSRC)
- Microsoft Security Engineering Center (MSEC)

Security Intelligence Report volume 8 (July - December 2009) – What's New
Guidance, advice and strategies

- Detailed strategies, mitigations and countermeasures
  - Fully revised and updated
  - Guidance on protecting networks, systems and people
- Microsoft IT 'real world' experience
  - How Microsoft IT secures Microsoft
- Malware patterns around the world with deep-dive content on 26 countries and regions

SIR v8 – The Security Intelligence Report
Data sources

- Malicious Software and Potentially Unwanted Software
  - MSRT has a user base of *more than 500 million* unique computers worldwide

Product Name	Main Customer Segment		Malicious Software		Spyware and Potentially Unwanted Software		Available at No Additional Charge	Main Distribution Methods
	Consumers	Business	Scan and Remove	Real-time Protection	Scan and Remove	Real-time Protection		
Windows Malicious Software Removal Tool	•		Prevalent Malware Families				•	WU/AU Download Center
Windows Defender	•				•	•	•	Download Center Windows Vista/ Windows 7
Windows Live OneCare safety scanner	•		•		•		•	Web
Microsoft Security Essentials	•		•	•	•	•	•	Web
Forefront Online Protection for Exchange		•	•	•				Web
Forefront Client Security		•	•	•	•	•		Volume Licensing

- Also data from **Bing** (billions of web page scans monthly), **Windows Live Hotmail** (more than 300 million active users, all mail scanned by Microsoft AV))
- New this time: **Microsoft Security Essentials**

SIRv8 Main Findings

SIRv8 Main Findings

- **Cybercrime** Continues to Mature, Mirroring Traditional Business Techniques
- Observing **security fundamentals**, combined with the **technology innovations** in products **developed with security goals in mind**, can help successfully mitigate attacks
- **Security is an industry-wide challenge**: No one individual, company, or technology can solve the challenges we face online today, so we need to work together to help create a **safer, more trusted Internet**

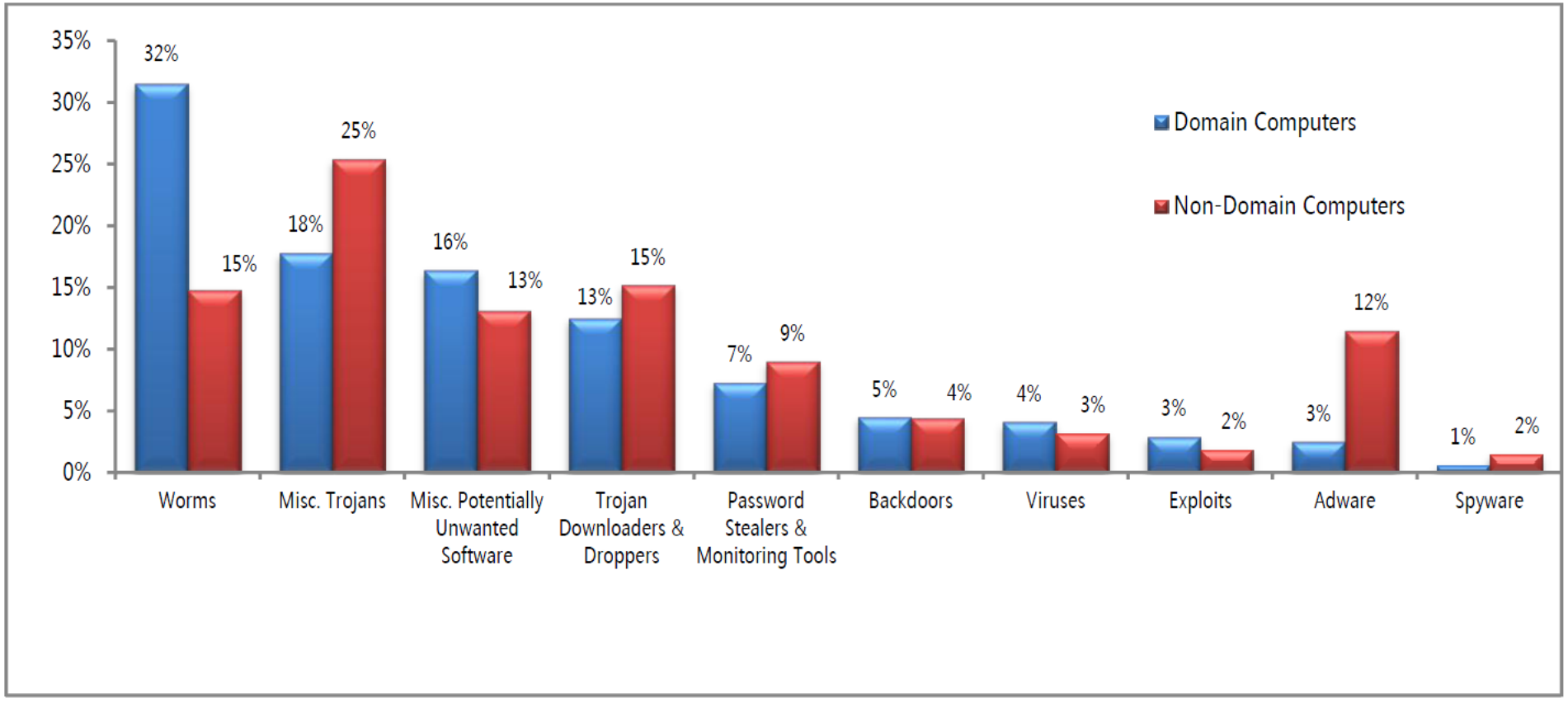
SIR v.8 New Findings - The Professionalism of Cybercrime

SIR v.8 New Findings - The Professionalism of Cybercrime

- Plenty of opportunities for criminals to exploit
  - 2,500 vulnerabilities reported by the software industry in 2H09
- Malware customized for attacks
  - Worms still biggest exploit for enterprise networks
  - Adware and Miscellaneous Trojans biggest threat to consumers
  - Rogue security software an issue for all, primarily consumers
- Criminals professional and organized
  - Specializing in and trading ‘services’ to maximize financial gain
  - Threats packaged and sold as “commodities”
  - Bot-herders offer ‘black cloud’ for hire

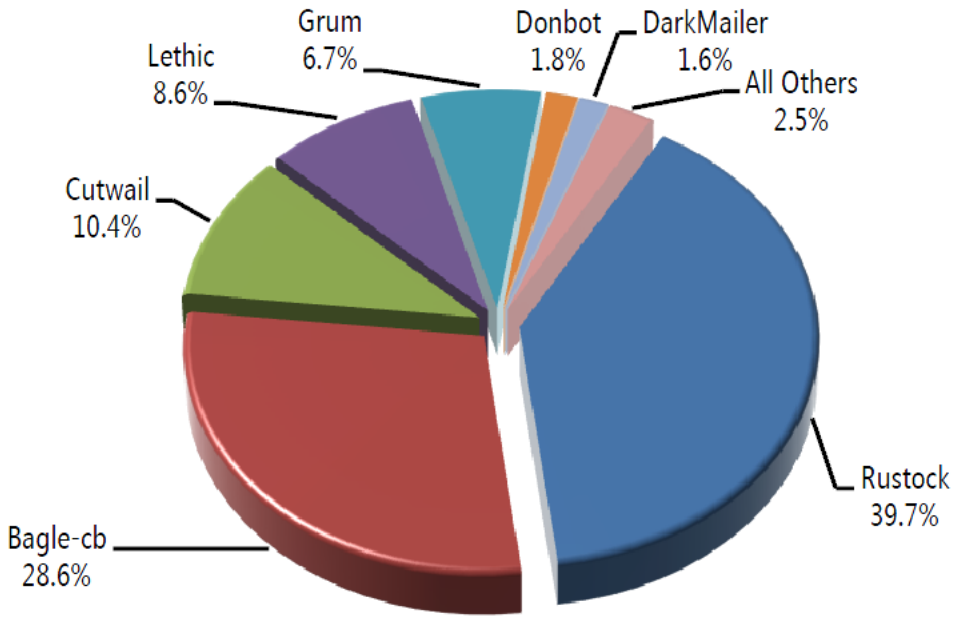
Malware customized for attacks

Threat category breakdown for domain-joined and non-domain computers in 2H09



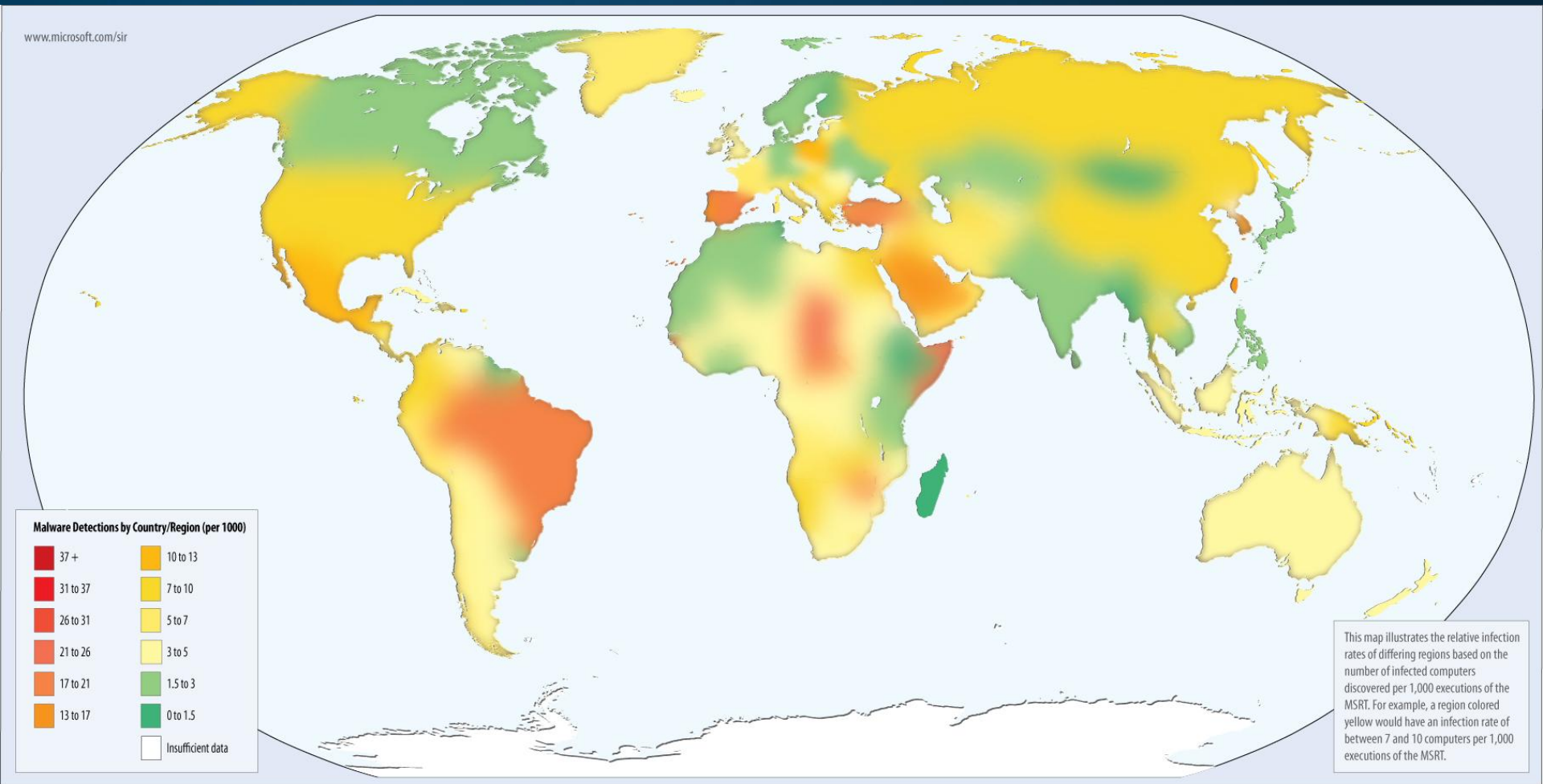
SPAM from Botnets

A few botnets are responsible for sending almost all of the botnet spam observed in 2H09



Malicious And Potentially Unwanted Software

Geographic distribution of malware – MSRT, 2H09



Worldwide malware infection rates

Lowest Infection Rates

Location	2H09
Réunion	1.3
Finland	1.4
Tunisia	1.4
Algeria	1.5
Belarus	1.5
Austria	1.7
Senegal	1.7
Philippines	1.7
Morocco	1.8
Vietnam	1.8

Highest Infection Rates

Location	2H09
Turkey	20.0
Brazil	18.0
Spain	17.1
Taiwan	16.7
Korea	16.0
Portugal	13.6
Saudi Arabia	13.0
Guatemala	12.5
Poland	11.0
Mexico	10.0

- Italy heat map infection rate (CCM) was 5.3 in 2H09, down from 6.9 in 1H09
  - i.e. 5.3 systems infected for every 1,000 systems MSRT executed on
- Lower than worldwide average of 7.0

Geographic Trends

- Italy's 20.0 percent decline is mostly the result of a steep decline in detections of the Trojan family Win32/Wintrim

	Country/Region	Computers Cleaned (2H09)	Computers Cleaned (1H09)	Change
1	United States	15,383,476	13,971,056	10.1% ▲
2	China	3,333,368	2,799,456	19.1% ▲
3	Brazil	2,496,674	2,156,259	15.8% ▲
4	United Kingdom	2,016,132	2,043,431	-1.3% ▼
5	Spain	1,650,440	1,853,234	-10.9% ▼
6	France	1,538,749	1,703,225	-9.7% ▼
7	Korea	1,367,266	1,619,135	-15.6% ▼
8	Germany	1,130,632	1,086,473	4.1% ▲
9	Canada	967,381	942,826	2.6% ▲
10	Italy	954,617	1,192,867	-20.0% ▼
11	Mexico	915,786	957,697	-4.4% ▼
12	Turkey	857,463	1,161,133	-26.2% ▼
13	Russia	677,601	581,601	16.5% ▲
14	Taiwan	628,202	781,214	-19.6% ▼
15	Japan	609,066	553,417	10.1% ▲
	Worldwide	41,024,375	39,328,515	4.3% ▲

Data from All Microsoft Security Products

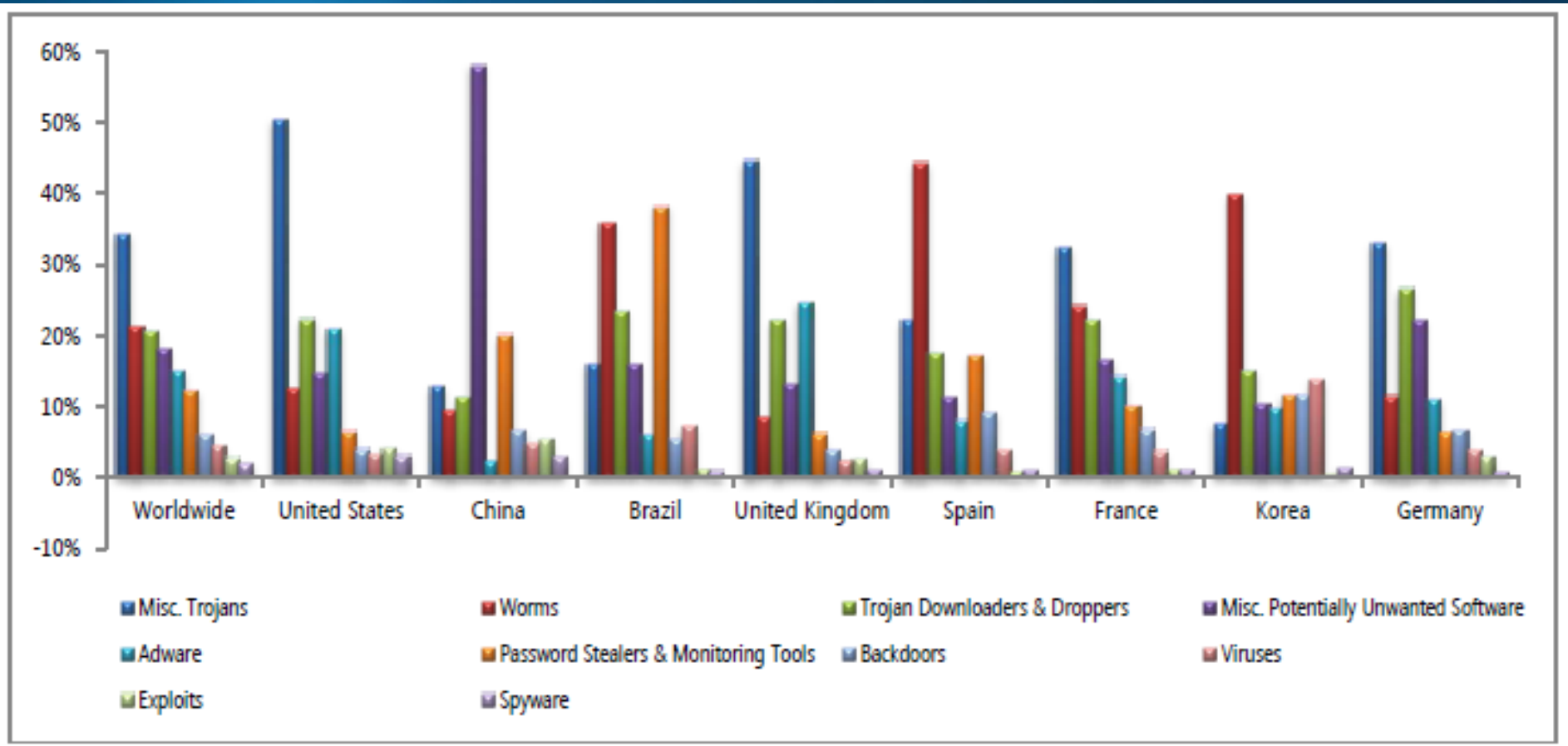
Top 25 Families worldwide in 2H09

	Family	Category	Infected computers
1	Win32/Taterf	Worms	3,921,963
2	Win32/Renos	Trojan Downloaders & Droppers	3,640,697
3	Win32/FakeXPA	Misc. Trojans	2,939,542
4	Win32/Alureon	Misc. Trojans	2,694,128
5	Win32/Conficker	Worms	1,919,333
6	Win32/Frethog	Password Stealers & Monitoring Tools	1,823,066
7	Win32/Agent	Misc. Trojans	1,621,051
8	Win32/BaiduSobar	Misc. Potentially Unwanted Software	1,602,230
9	Win32/GameVance	Adware	1,553,646
10	Win32/Hotbar	Adware	1,476,838
11	Win32/Yektel	Misc. Trojans	1,377,123
12	ASX/Wimad	Trojan Downloaders & Droppers	1,306,644

Rank	Family	Category	Infected computers
13	Win32/ZangoSearch Assistant	Adware	1,235,666
14	Win32/FakeSpypro	Misc. Trojans	1,193,737
15	Win32/Hamweq	Worms	967,436
16	Win32/Bancos	Password Stealers & Monitoring Tools	963,221
17	Win32/Winwebsec	Misc. Trojans	947,781
18	Win32/Vundo	Misc. Trojans	935,087
19	Win32/Autorun	Worms	754,168
20	Win32/Koobface	Worms	753,695
21	Win32/PossibleHosts FileHijack	Misc. Potentially Unwanted Software	730,019
22	Win32/Zlob	Trojan Downloaders & Droppers	670,924
23	Win32/C2Lop	Misc. Trojans	654,017
24	Win32/Bredolab	Trojan Downloaders & Droppers	635,277
25	Win32/DoubleD	Adware	630,965

Worldwide Threat Categories

- Common theme: localized threats



Rogue Security Software

- Cleaned on 7.8 million computers in 2H09, up from 5.3 million computers in 1H09—an increase of 46.5 percent, which suggests that rogue security software provides its distributors with large payoffs
- Three new consumer-oriented videos have been posted on http://www.microsoft.com/protect
- Italy is still not heavily affected due to the current lack of localized versions

The Italian View

Data from All Microsoft Security Products

Top 25 Families in Italy in 2H09

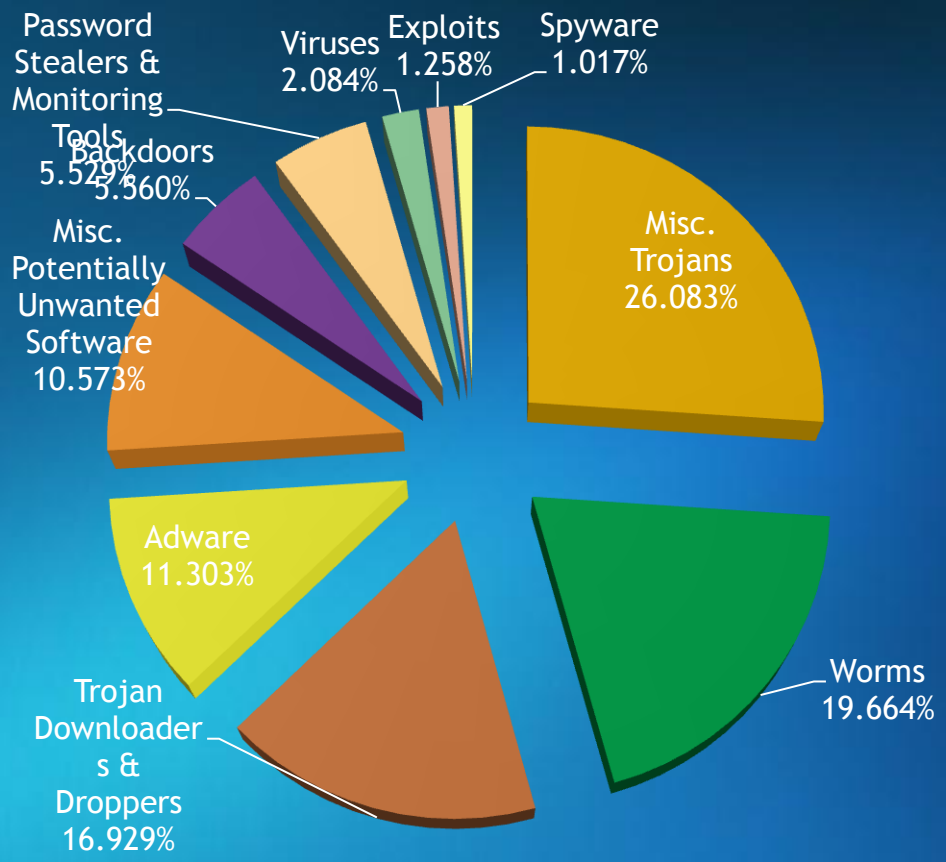
	Family	Category	Infected computers
1	Win32/Conficker	Worms	102,623
2	Win32/Alureon	Misc. Trojans	92,419
3	Win32/Renos	Trojan Downloaders & Droppers	84,733
4	Win32/Taterf	Worms	83,771
5	Win32/Hotbar	Adware	63,142
6	Win32/Vundo	Misc. Trojans	51,483
7	Win32/Wintrim	Misc. Trojans	46,922
8	Win32/C2Lop	Misc. Trojans	44,356
9	Win32/Frethog	Password Stealers & Monitoring Tools	37,324
10	ASX/Wimad	Trojan Downloaders & Droppers	34,600
11	Win32/DoubleD	Adware	26,805
12	Win32/Agent	Misc. Trojans	23,770

Rank	Family	Category	Infected computers
13	Win32/ZangoSearchAssistant	Adware	22,127
14	Win32/FakeCog	Miscellaneous Trojans	22,075
15	Win32/Bagle	Worms	20,745
16	Win32/Skintrim	Miscellaneous Trojans	20,593
17	Win32/IRCbot	Backdoors	17,081
18	Win32/Winwebsec	Miscellaneous Trojans	17,079
19	Win32/Rustock	Backdoors	15,206
20	Win32/Autorun	Worms	14,848
21	Win32/Cutwail	Trojan Downloaders & Droppers	14,797
22	Win32/Zlob	Trojan Downloaders & Droppers	14,241
23	Win32/Hamweq	Worms	14,100
24	Win32/FakeXPA	Miscellaneous Trojans	13,724
25	Win32/RealVNC	Misc. Potentially Unwanted Software	12,874

Top Threats in Italy

Disinfected Threats by Category in 2H09

Category	Infected Computers	Trend from 1H09
Miscellaneous Trojans	322,299	-47,66%
Worms	242,982	+2,42%
Trojan Downloaders & Droppers	209,182	+26,44%
Adware	139,670	-16,14%
Misc. Potentially Unwanted Software	130,646	-11,72%
Backdoors	68,697	+30,84%
Password Stealers & Monitoring Tools	68,316	+7,45%
Viruses	25,745	+76,37%
Exploits	15,550	+182,68%
Spyware	12,570	-50,19%



Top Threats in Italy in 2H09
Prevalent Families - Summary

- Of the top families:
  - 9 of the top 10 were malware, only 1 was potentially unwanted software, such as adware
  - 21 out of the top 25 families were malware

Top Threats in Italy in 2H09
Prevalent Families - Detail

- Win32/Conficker was the #1 threat in Italy, #5 worldwide
  - A worm that infects computers across a network by spreading via removable hard drives, exploiting weak passwords on file shares, or exploiting a vulnerability in the Windows Server service. Infection can result in remote code execution when file sharing is enabled. The worm also disables important system services and some security products and may download arbitrary files.

Top Threats in Italy in 2H09
Prevalent Families - Detail

- Win32/Alureon was #2 in Italy, #4 worldwide
  - A family of data-stealing trojans which allow an attacker to intercept incoming and outgoing Internet traffic in order to gather confidential information such as user names, passwords, and credit card data. May also allow an attacker to transmit malicious data to the infected computer. May modify DNS settings on the host computer to enable the attacker to perform these tasks.

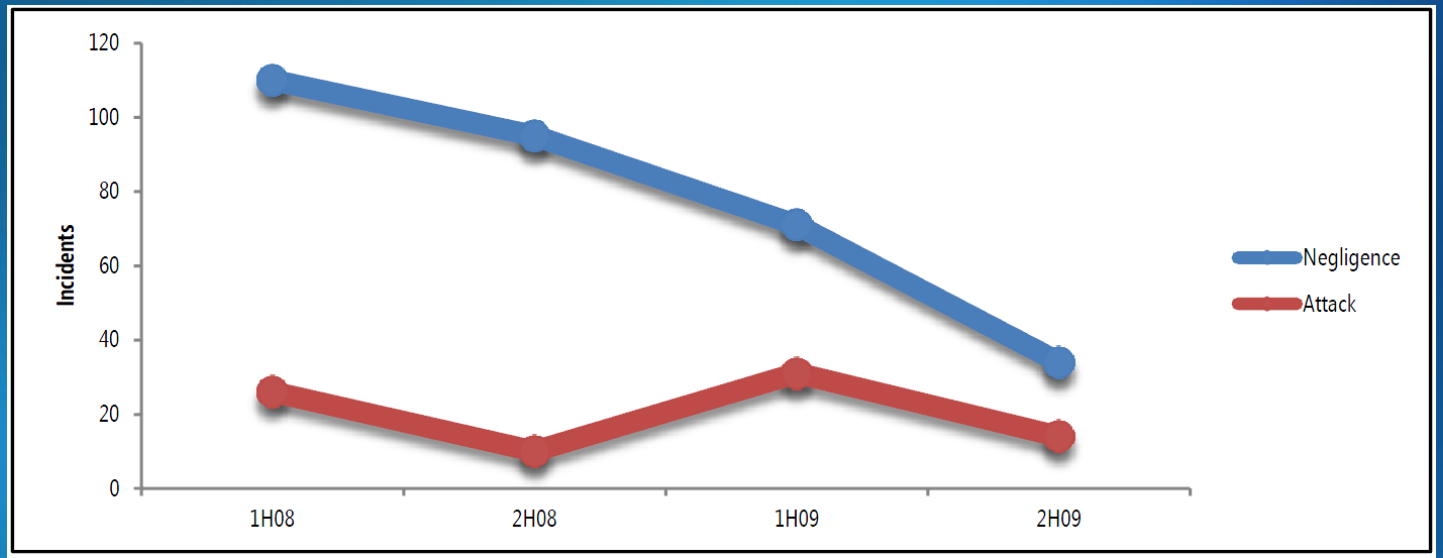
Top Threats in Italy in 2H09
Prevalent Families - Detail

- Win32/Renos was the #3 threat in Italy and #2 worldwide
  - Automatically downloads several potentially unwanted software families. These programs typically present erroneous warnings claiming the system is infected with spyware and offer to remove the alleged spyware for a fee. In some cases, the programs may also cause system instability.
- Win32/Taterf was #4 threat in Italy, #1 worldwide
  - A family of worms that spread via mapped drives in order to steal login and account details for popular online games.

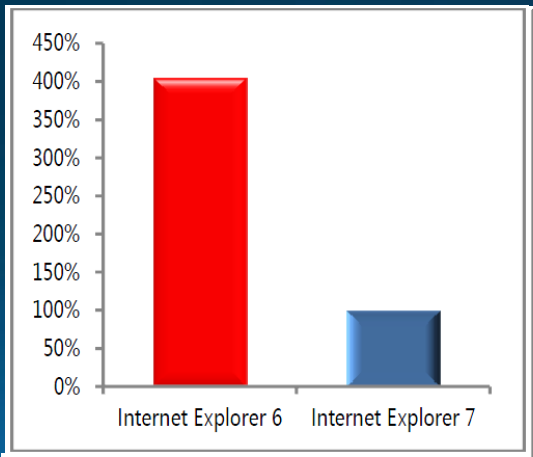
Advancements in Software Protection and Development

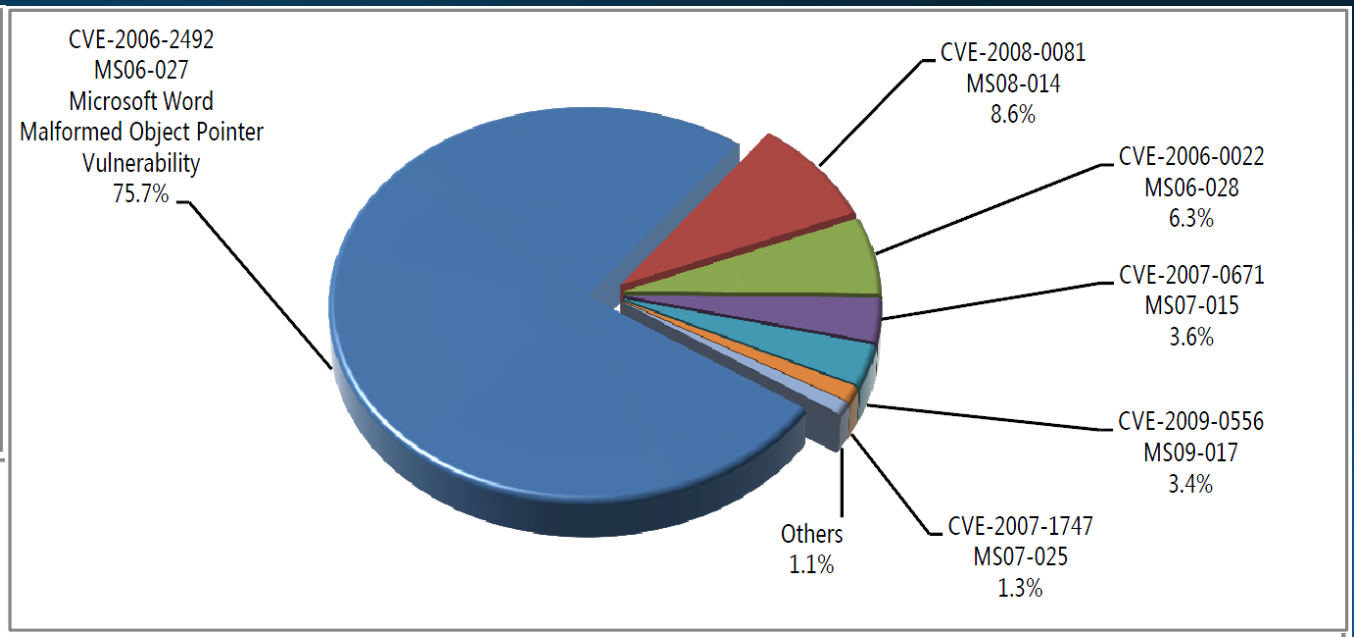
Advancements in Software Protection Raising the Bar on Cybercrime –

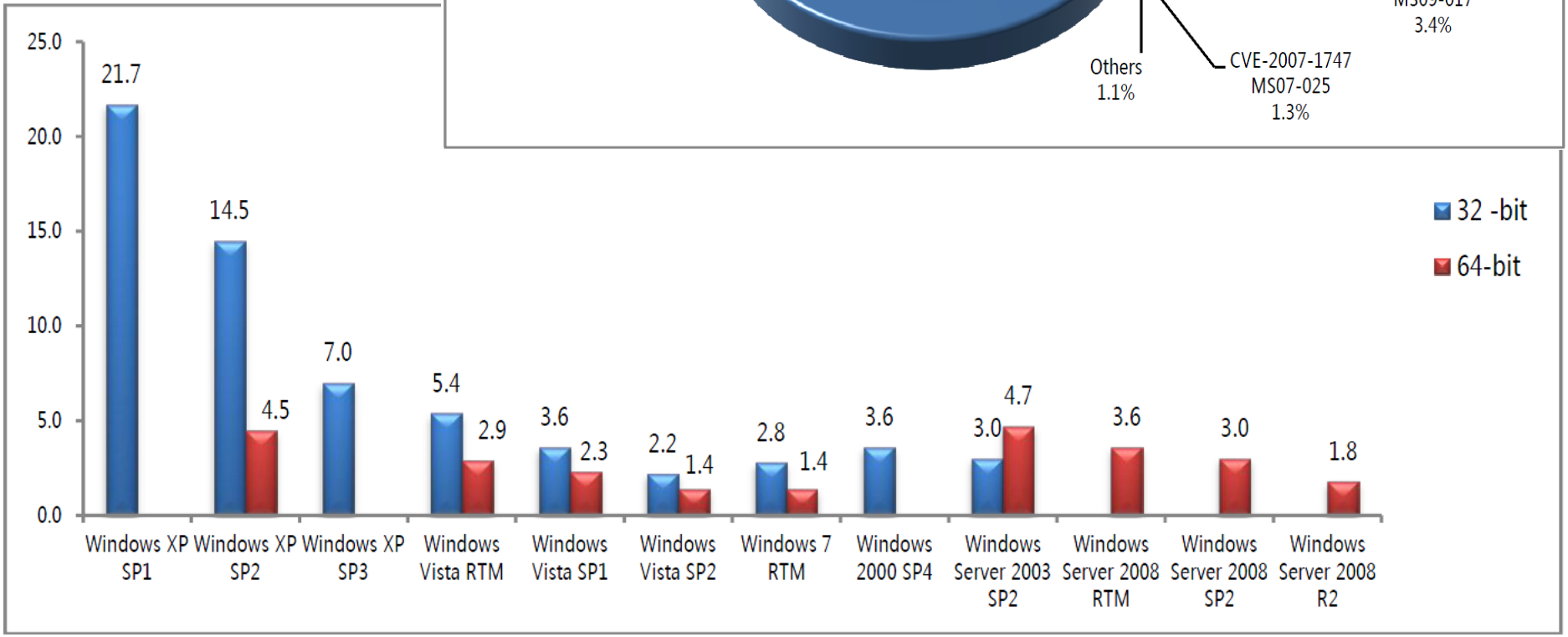
- Newer software keeps up with attacks
  - Windows
  - Internet Explorer
  - Search technology
- People and lost/stolen devices at greater risk than software



Newer Software Better Defense





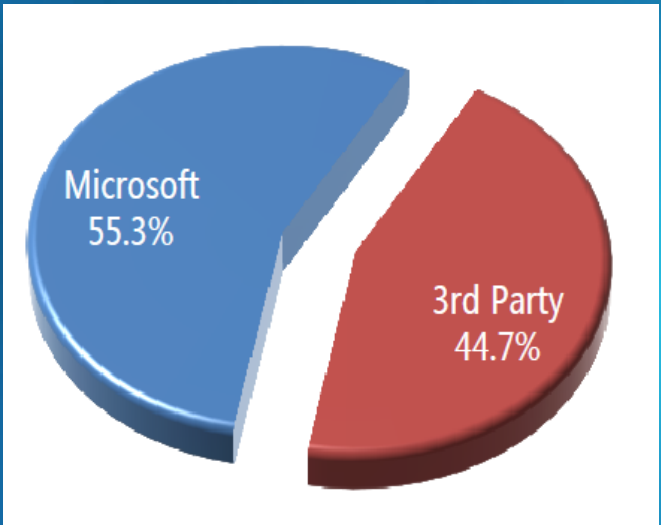


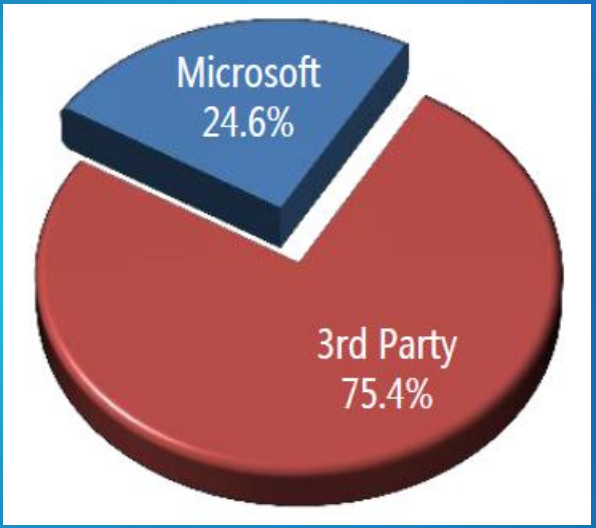
Security is an industry-wide challenge

Advancements in Software Development- Raising the Bar on Cybercrime

- Microsoft SDL proven effective at Microsoft
  - Reduced number and severity of vulnerabilities in Microsoft platform and products

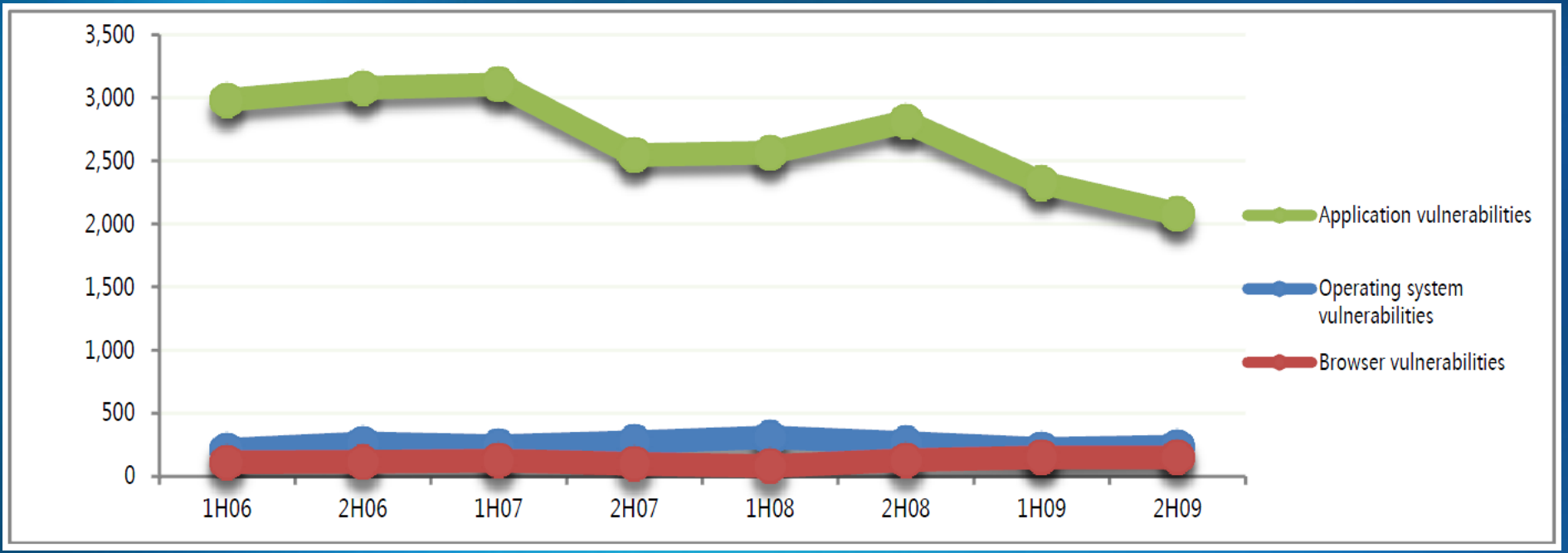
- As Windows gets 'harder' attackers move targets
  - 95% of SIRv8 vulnerabilities in third party applications
  - 55,3% of the most exploited browser-based vulnerabilities on Windows XP exist in third party applications, 75,4% on Windows Vista/Windows 7





The Importance of Secure Coding Best Practices

Industry-wide operating system, browser, and application vulnerabilities, 1H06–2H09



What the Users and Industry Can Do

What the Users Can Do

- Consumers' Security Best Practices are still valid
  - Educate on security-conscious behavior and learn new threats
  - Use newer software as much as possible
  - Keep ALL software up to date with the latest security updates
  - Use a trusted up-to-date antimalware application
  - Use a firewall application
- www.microsoft.com/protect

What the Industry Can Do

From Microsoft CISO Bret Arsenault

- Protect your network and systems - Security best practices remain effective
  - Defense in Depth
  - Migrate from old software
  - Regular updates

- Protect your people
  - Educate on security-conscious behavior and best practices
  - Lock devices and laptops – i.e.Bitlocker Drive Encryption

- Develop with SDL - expertise available to all
  - 80,000 downloads of10 sets of guidance and materials
  - 50,000 downloads of four security developer tools
  - SDL Pro Network
  - www.microsoft.com/sdl

SIRv8 Main Findings

- **Cybercrime** Continues to Mature, Mirroring Traditional Business Techniques
- Observing **security fundamentals**, combined with the **technology innovations** in products **developed with security goals in mind**, can help successfully mitigate attacks
- **Security is an industry-wide challenge**: No one individual, company, or technology can solve the challenges we face online today, so we need to work together to help create a **safer, more trusted Internet**