
HP Security Services
HITB SECCONF 2007 - DUBAI
2ND - 5TH APRIL 2007 - SHERATON CREEK HOTEL
DEEP KNOWLEDGE SECURITY CONFERENCE

symantec™

Confidence in a connected world.

Global SOCs – Threat Insight & Findings – HiTB – Final Version

Ivor Rankin

Principle Security Consultant

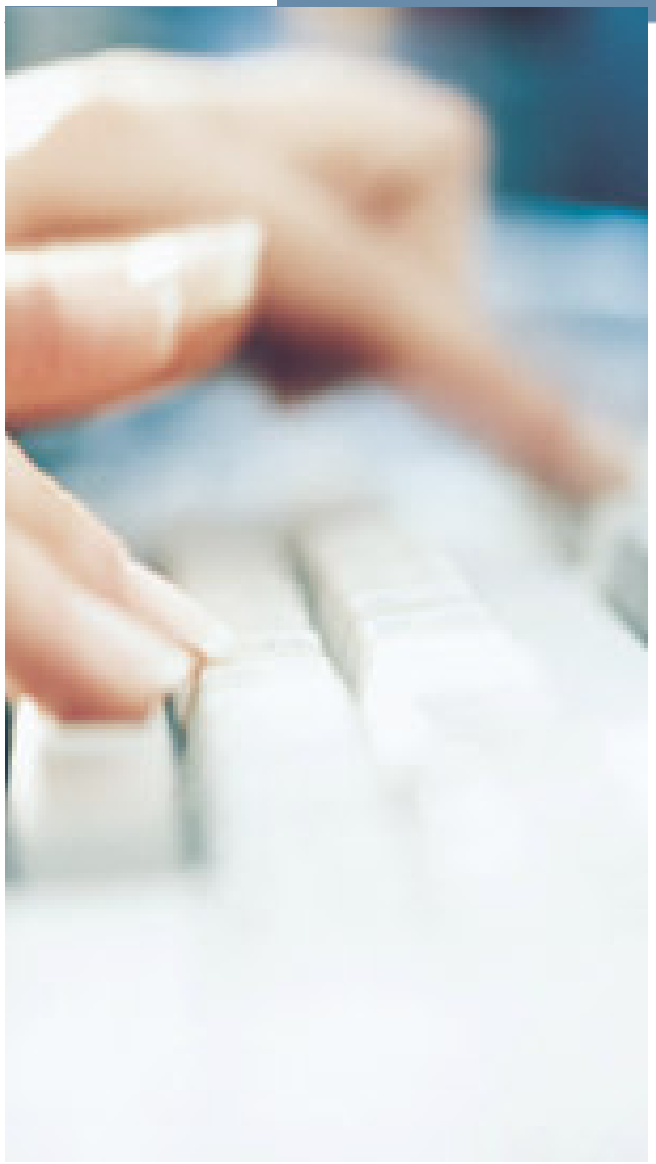
EMEA - Forensics & IRH Center Of Excellence

hp® invent

Thoughts On IT Security

- You're not here to learn about IT Security….you're here to learn how to learn about IT security

- Four Steps To Knowledge Lifecycle:
  1. Subconcious Incompetence
  2. Concious Incompetence
  3. Counscious Competence
  4. Subconscious Competence
  5. Attend HiTB
  6. Goto: Step 1



Agenda

- Introducing HP Security Services
- HP & Symantec Strategic Security Alliance
- Stats, Surveys & Just The Facts
- Global Internet Security Threat Report Findings
- Key Facts and Figures
  - Attacks
  - Vulnerabilities
  - Malicious Code
  - Phishing, Spam & Security Risks
  - Future Watch
- GCC Regional Attack Trends & Analysis
- … A Word From Our Sponsors

HP Security Services Vision

> “To be the best at helping customers safeguard their information and assets through the management of IT related risk.”

HP Security Solutions Partnership

Enterprise Security Solutions

- Assessing, planning, design, implementation and rollout of a proactive security solution around HP & Symantec Security Products

Compliance management	Security information management	Endpoint security	E-mail security & retention
Demonstrate due care to internal and external auditors with dashboard views that display percentage of compliance across the enterprise.	Real-time global security intelligence to proactively detect, remediate and measure ongoing threats	Centrally managed policy definition enforced by an agent on endpoint to ensure protection and compliance before network access is granted	Increases the security of information by stopping unwanted e-mail and effectively archiving and retrieving messages

Internet Security Threat Report XI
Key Metrics

Attacks:

- Malicious activity by country
- Data breaches
- Underground economy servers

Vulnerabilities:

- Severity
- Zero-day
- Database
- Vendor responsiveness

Malicious Code:

- Potential infections
- Malicious code that exploits vulnerabilities

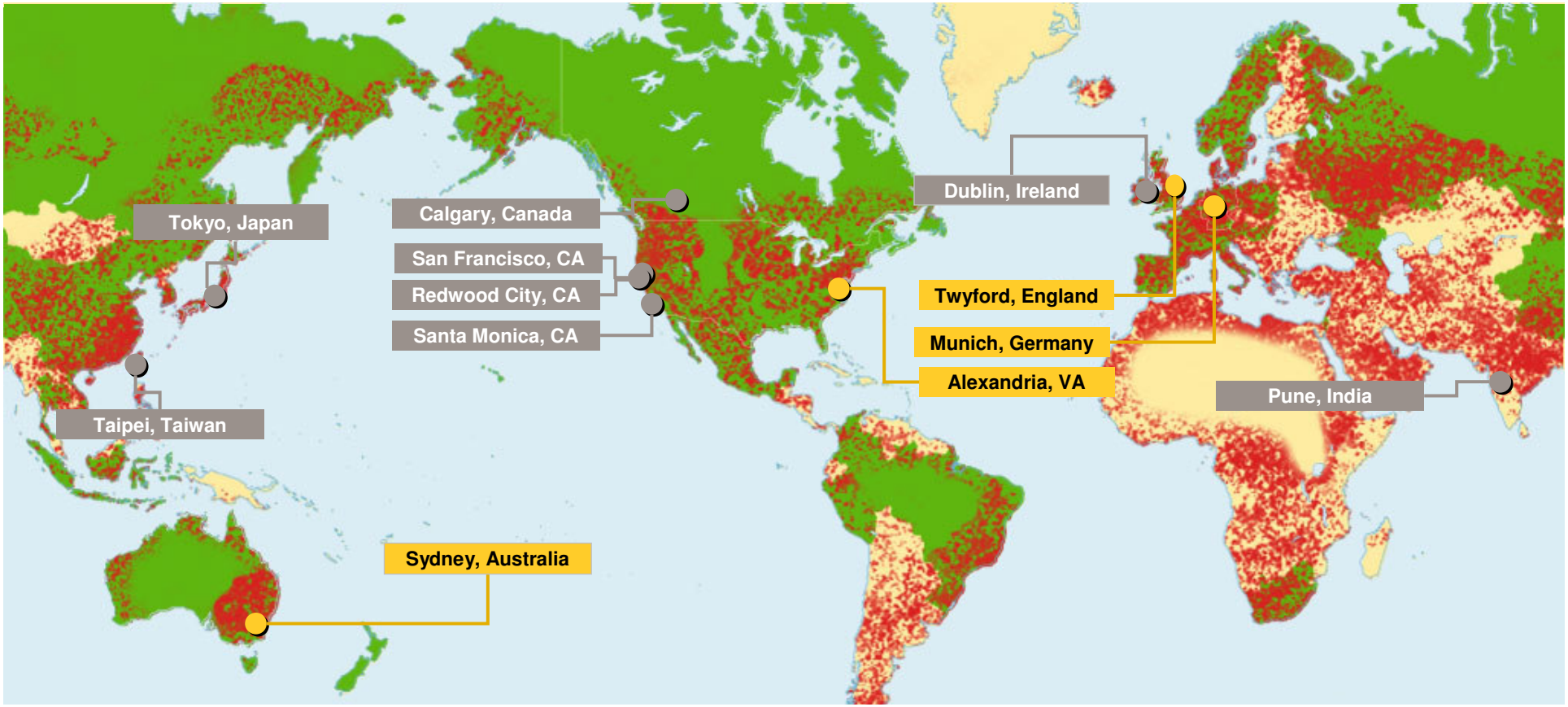
Phishing, spam and security risks:

- Daily and seasonal variations in phishing activity
- Top countries hosting phishing sites
- Top countries hosting spam zombies

THE Source: Symantec Global Intelligence Network

4 Symantec SOCs + 74 Symantec Monitored Countries + 40,000+ Registered Sensors in 180+ Countries + 8 Symantec Security Response Centers

>6,200 Managed Security Devices + 150 Million Systems Worldwide + 35% of World's email Traffic + Advanced Honeypot Network



Internet Security Threat Report XI Important Facts

- Data Sources
  - Symantec Global Intelligence Network
    - 40,000 registered sensors in 180 countries.
    - 120 million desktop, gateway and server antivirus installations.
    - 20,000 vulnerabilities in the Symantec vulnerability database.
    - 2,000,000 decoy accounts in the Symantec Probe Network - 30% of all email traffic
  - Symantec Global Coverage
    - 4 Security Operations Centers, 8 Symantec Research Centers.
    - 1800 analysts, 6200 managed security devices.
    - Symantec software protects more than 370 million computers or email accounts worldwide, and 99% of the Fortune 500 & 1000 utilize Symantec products.
- What the ISTR is:
  - A detailed report on trends that ***Symantec*** sees.
  - Based on real, ***empirical*** data collected by the Global Intelligence Network.
  - Only publicly available report to offer a ***complete*** view of the current Internet security landscape.
  - Identifies and ***analyzes*** attacker methods and preferences.
  - Vendor ***neutral.***
- What the ISTR is not:
  - A ***survey*** of opinions.
  - Product driven ***marketing.***
  - Scientific ***certainty.***

Key Messages

- The current threat environment is characterized by an increase in data theft, data leakage, and the creation of malicious code that targets specific organizations.
- Attackers are refining their methods and consolidating assets to create global networks that support coordinated criminal activity
- Increased inter-operability between diverse threats - blended threats +
- Year of the zero-day, targeted malicious code and the exploitation of medium severity vulnerabilities
- High levels of malicious activity across the Internet with increases in bot networks, phishing, spam and trojans

symantec™

Confidence in a connected world.

Internet Security Threat Report Volume XI
Key Facts and Figures – With GCC Insights

hp® invent

Top Attacking GCC Countries

Top Attacking Countries

Rank	GCC	Description	SUB-REGION
46	1	**United Arab Emirates**	Middle-east
61	2	**Saudi Arabia**	Middle-east
64		**Iran**	Middle-east
65	3	**Kuwait**	Middle-east
76	4	**Bahrain**	Middle-east
78	5	**Qatar**	Middle-east
93	6	**Oman**	Middle-east

Top Targetted Countries - GCC

Rank	GCC Rank	Description	SUB-REGION
46	1	United Arab Emirates	Middle-east
62	2	Saudi Arabia	Middle-east
69	3	Qatar	Middle-east
79	4	Bahrain	Middle-east
86	5	Kuwait	Middle-east
93	6	Oman	Middle-east

Attack Trends
Malicious Activity

- Between July 1st and December 31st the United States was the top country for malicious activity (raw numbers) with 31% of the overall proportion. China was ranked second with 10%.
- When accounting for Internet populations, Israel was the top country with 9% followed by the Taiwan region with 8%. Six of the top ten countries in this metric were located in EMEA.

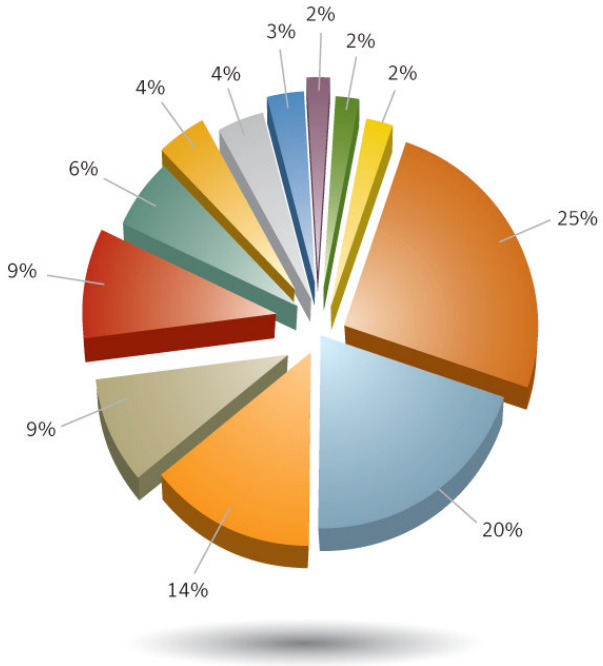
Overall Rank	Country	Overall Proportion	Malicious Code Rank	Spam Host Rank	Command and Control Server Rank	Phishing Host Rank	Bot Rank	Attack Rank
1	United States	31%	1	1	1	1	2	1
2	China	10%	3	2	4	8	1	2
3	Germany	7%	7	3	3	2	4	3
4	France	4%	9	4	14	4	3	4
5	United Kingdom	4%	4	13	9	3	6	6
6	South Korea	4%	12	9	2	9	11	9
7	Canada	3%	5	23	5	7	10	5
8	Spain	3%	13	5	15	16	5	7
9	Taiwan	3%	8	11	6	6	7	11
10	Italy	3%	2	8	10	14	12	10

Attack Trends
Malicious Activity - GCC

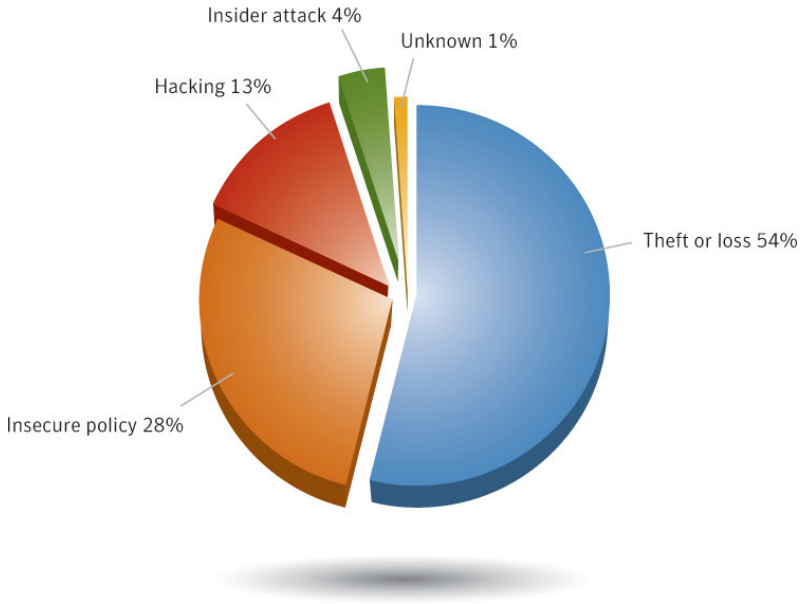
Rank	GCC	Country	SUB-REGION
46	**1**	Kuwait	Middle-east
47	**2**	Jordan	Middle-east
60	**3**	United Arab Emirates	Middle-east
62	**4**	Saudi Arabia	Middle-east
82	**5**	Bahrain	Middle-east
91	**6**	Qatar	Middle-east

Attack Trends
Data Breaches

- Information on data breaches that ***could*** lead to identity theft. Data collected is **not** Symantec data.
- The government sector accounted for the majority of data breaches with 25%, followed by Education (20%) and Healthcare (14%) - the majority of breaches (54%) were due to theft or loss with hacking only accounting for 13%.



- Government 25%
- Education 20%
- Health care 14%
- Financial services 9%
- Other 9%
- Insurance 6%
- Military 4%
- Retail and wholesale and e-commerce 4%
- Telecommunications 3%
- Biotech/pharmaceutical 2%
- Law enforcement 2%
- Transportation 2%



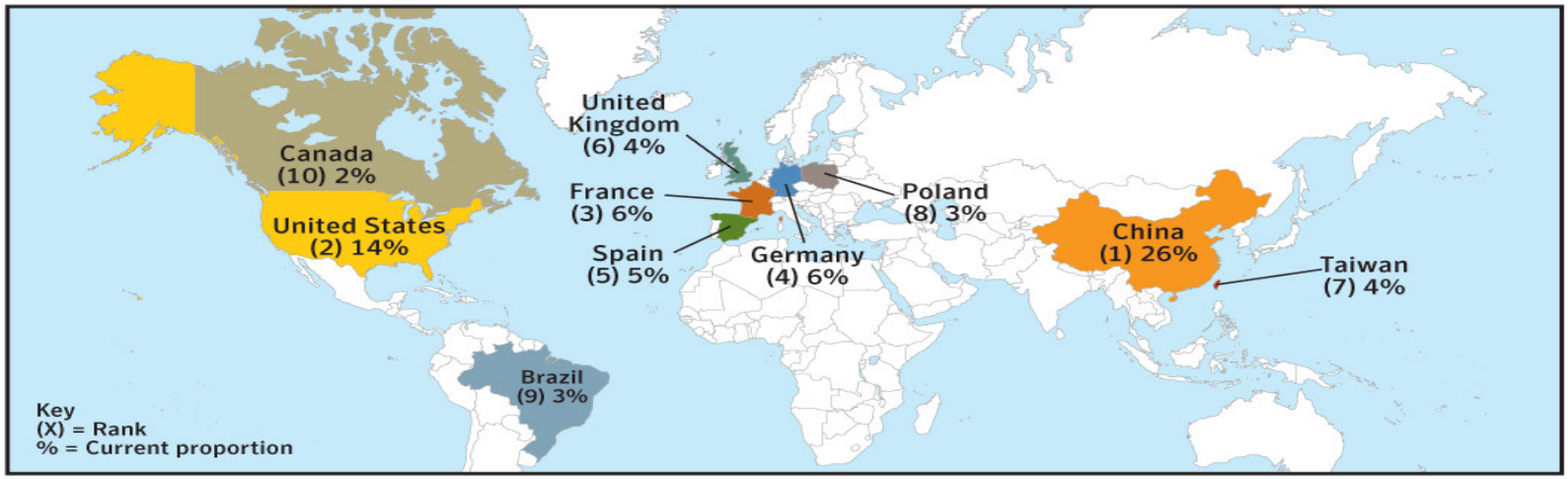
Attack Trends
Underground Economy Servers

- Trading in credit cards, identities, online payment services, bank accounts, bots, fraud tools, etc.
- Ranked according to geographic location of the server and the location of banks.
- The United States had the highest proportion of underground economy servers that Symantec observed with 51%. 7 of the top ten were located in EMEA.
- 86% of banks whose credit cards were stolen were located in the United States followed by the United Kingdom (7%) and Canada (1%).

Item	Advertised Price (in US Dollars)
United States-based credit card with card verification value	$1–$6
United Kingdom-based credit card with card verification value	$2–$12
An identity (including US bank account, credit card, date of birth, and government issued identification number)	$14–$18
List of 29,000 emails	$5
Online banking account with a $9,900 balance	$300
Yahoo Mail cookie exploit—advertised to facilitate full access when successful	$3
Valid Yahoo and Hotmail email cookies	$3
Compromised computer	$6–$20
Phishing Web site hosting—per site	$3–5
Verified PayPal account with balance (balance varies)	$50–$500
Unverified PayPal account with balance (balance varies)	$10–$50
Skype account	$12
World of Warcraft account—one month duration	$10

Attack Trends
Bot Networks

- During the current reporting period Symantec observed an average of 63,912 active bot network computers per day, an 11% increase over the first half of the year. The worldwide total of distinct bot-infected computers that Symantec identified rose to just over 6,049,594 - a 29% increase.
- Command and control servers decreased during this period to 4,746 - a 25% decrease. The United States continues to have the highest number of command and control servers worldwide with 40% - a 2% drop from it's previous total.
- China has increased its global proportion of bot-infected computers to 26% while the United States continues to decline. EMEA countries, with the exception of the U.K., showed the largest increase.



Attack Trends
Bot Networks - GCC

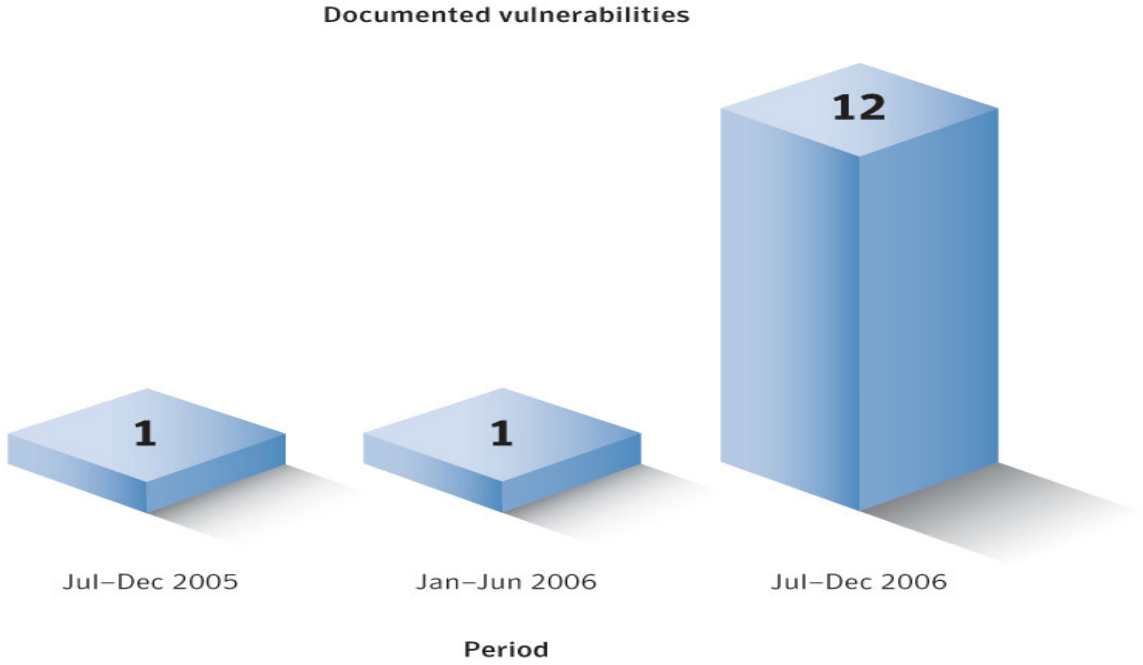
Rank	GCC	Description	SUB-REGION
46	1	United Arab Emirates	Middle-east
61	2	Saudi Arabia	Middle-east
64		Iran	Middle-east
65	3	Kuwait	Middle-east
76	4	Bahrain	Middle-east
78	5	Qatar	Middle-east
93	6	Oman	Middle-east

Attack Trends
Additional Metrics

- The United States was the top country of attack origin accounting for 33% of worldwide attack activity.
- The United States was the target of most denial of service attacks (54%) and Government was the most targeted sector for DoS attacks at 37%.
- Home users continue to be the most targeted sector accounting for 93% of all targeted attacks.

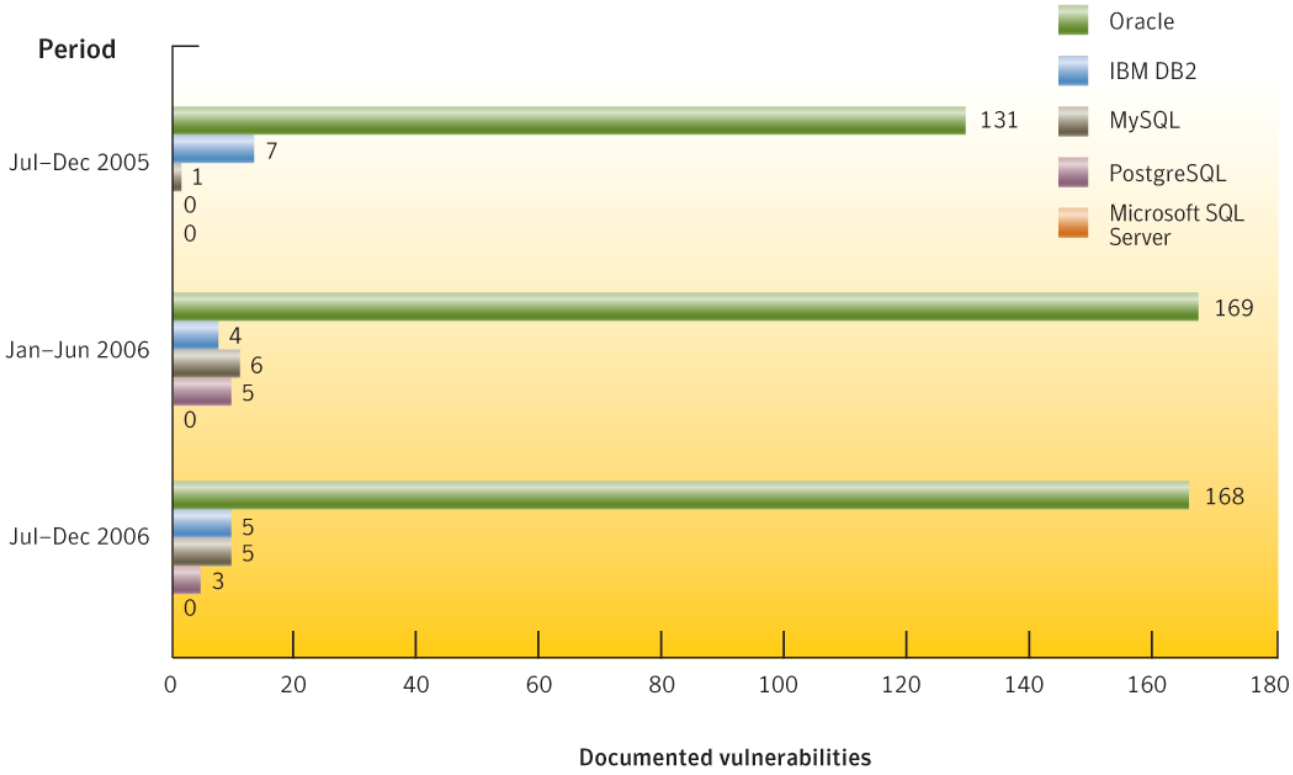
Vulnerability Trends
Zero-day

- Key Definition: “A zero-day vulnerability is one for which there is sufficient public evidence to indicate that the vulnerability has been exploited in the wild prior to being publicly known.”
- From July 1st - December 31st 2006, Symantec documented 12 zero-day vulnerabilities, a significant increase over the previous two reporting periods.
- In September, four zero-day vulnerabilities were documented, the majority of which affected office applications, Internet Explorer and ActiveX controls.



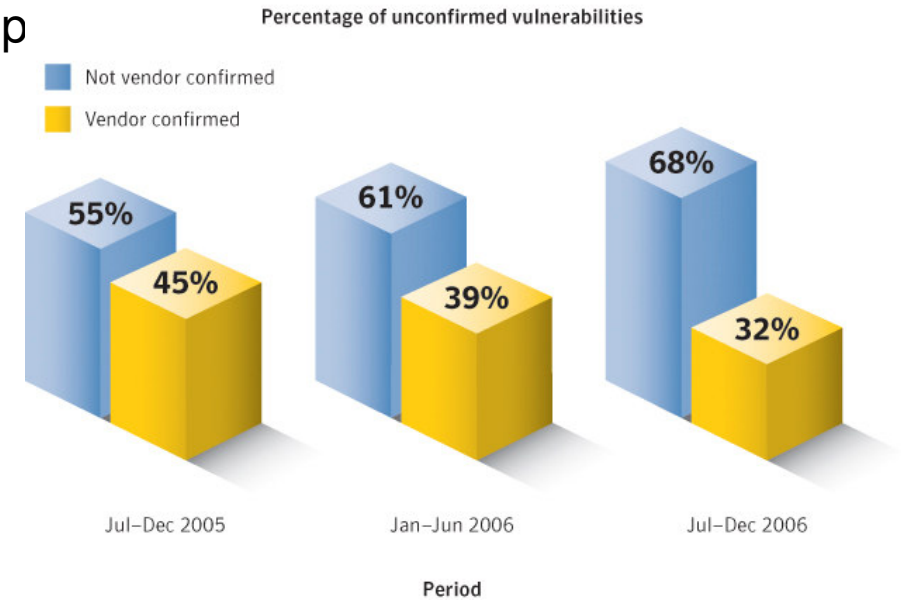
Vulnerability Trends Databases

- Oracle databases have the highest number of documented vulnerabilities of the major database vendors - 168.
- Microsoft SQL has not had *any* documented vulnerabilities in the past three reporting periods.



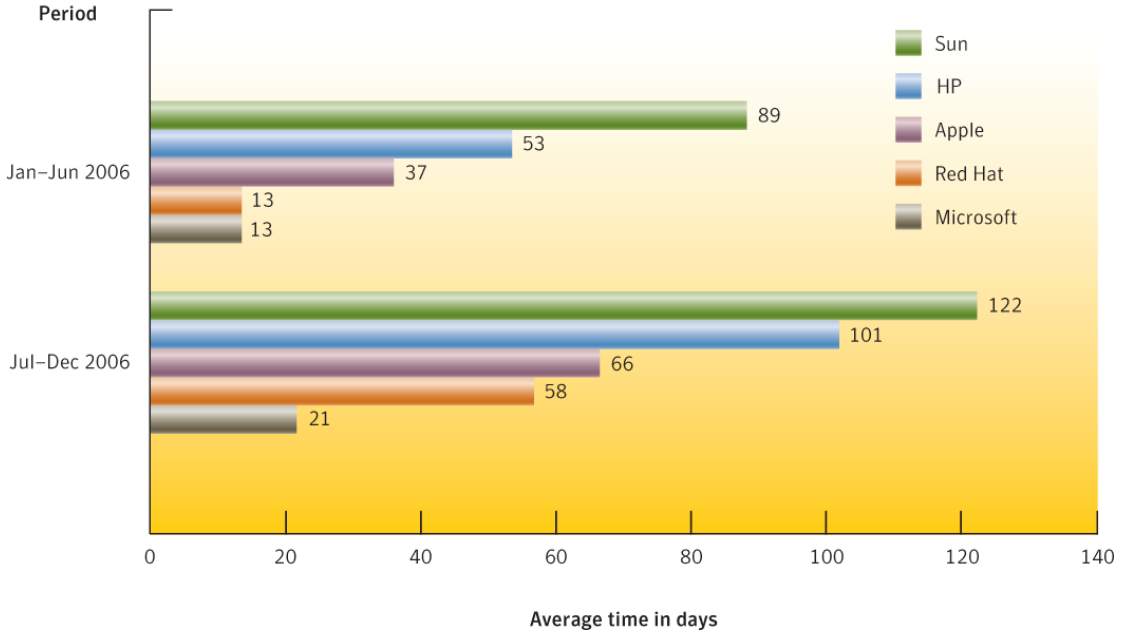
Vulnerability Trends
Vendor Responsiveness

- Key definition: “Vendor responsiveness is measured by the proportion of vulnerabilities that remains unconfirmed by the vendor, and therefore un-patched, over time.”
- In the current reporting period, 68 percent of documented vulnerabilities were not confirmed by the affected vendor, an increase from 61% the previous reporting p



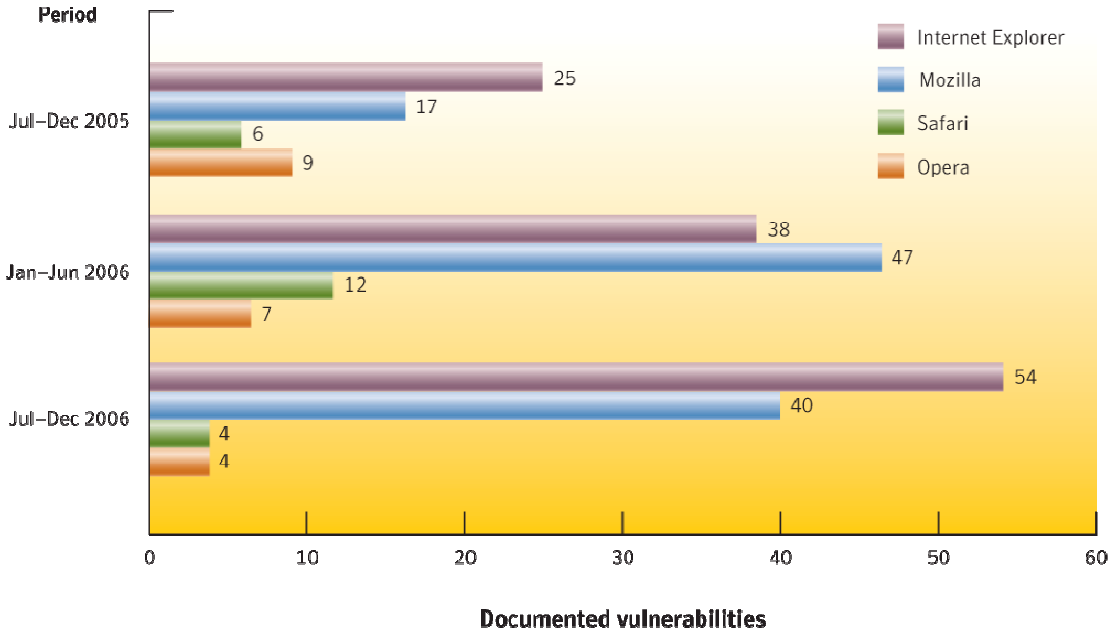
Vulnerability Trends
Patch Development Time

- All vendors reported longer average patch development times. Sun had the longest patch development times with 122 days respectively. Microsoft had the shortest patch development time with 21 days.
- The majority of vulnerabilities are medium severity and affect 3rd party components. Microsoft had the highest number of severe vulnerabilities with 12.
- As with previous periods, Microsoft Windows was the operating system that had the most vulnerabilities with associated exploit code and exploit activity in the wild.



Vulnerability Trends
Browser Vulnerabilities and W.O.E.

- IE was the most targeted browser with 77% of all targeted attacks.
- Microsoft had the highest number of documented vulnerabilities with 54 followed by Mozilla with 40. Microsoft was the only vendor to have a documented high severity browser vulnerability and the only vendor to increase its vulnerability count.
- Mozilla had the shortest window of exposure with 2 days followed by IE with 10 days.

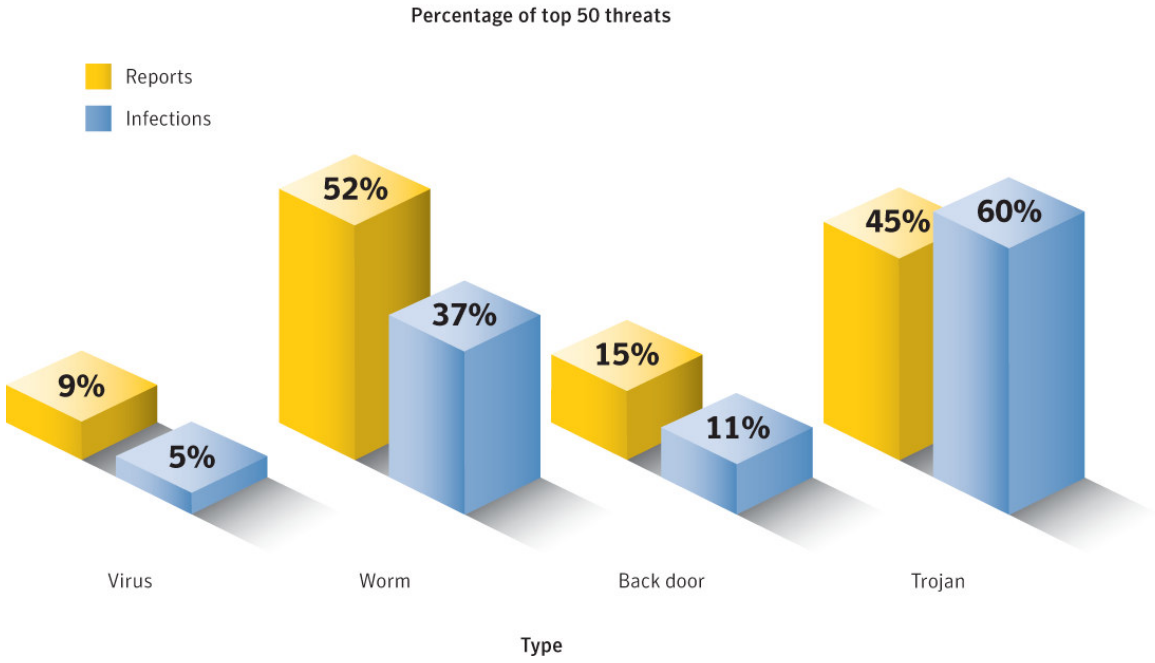


Vulnerability Trends
Additional Metrics

- Symantec documented 2,526 vulnerabilities in the current reporting period, 12% higher than the previous reporting period.
- Severity classification: High severity 4%, Medium severity 69% and Low severity 27%.
- Web applications constituted 66% of all documented vulnerabilities. 77% of easily exploitable vulnerabilities affected web applications.
- 79% of all vulnerabilities were considered easily exploitable, 94% of which were remotely exploitable.
- The W.O.E. for enterprise vendors was 47 days. Average exploit development time of 5 days and average patch development of 52 days.
- 25% of exploit code was released less than one day after the publication of a vulnerability. 31% was released between one and six days.

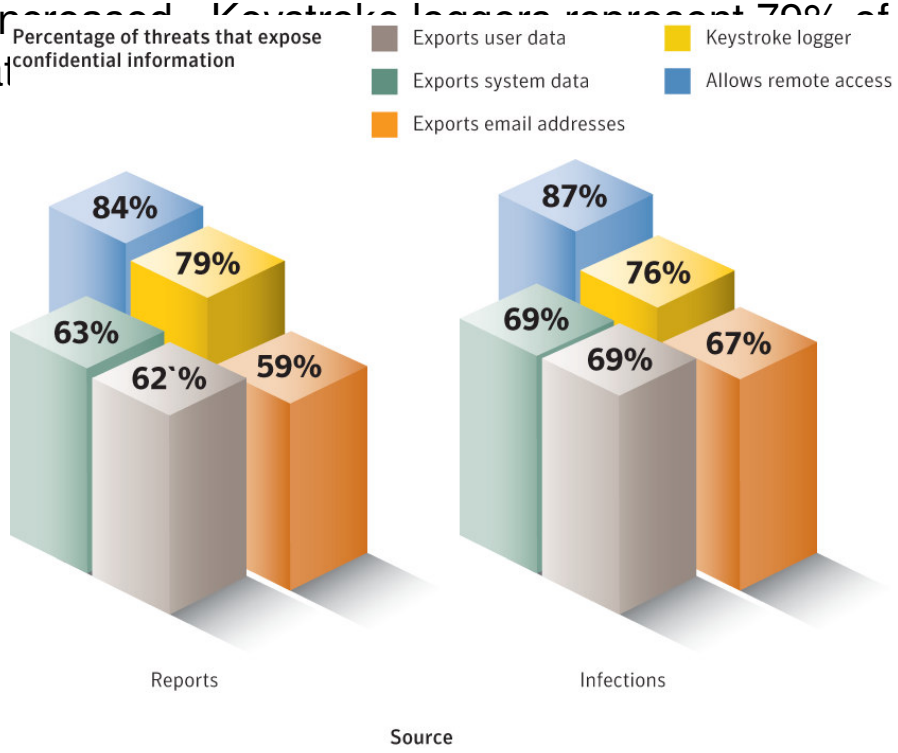
Malicious Code Trends
Types

- Introduction of proprietary technology that provides a comparison between reports (volume) and ***potential/attempted*** infections. In some cases, a threat may be widely reported but not cause a wide number of infections and vice versa.
- Supports Symantec's assertion that Trojans are on the rise and may constitute a greater threat because they tend to exploit web browser and zero-day vulnerabilities. Trojans reported to Symantec increase from 23% in the last reporting period to 45% in the current period and represent 60% of malicious code by potential/attempt infections.



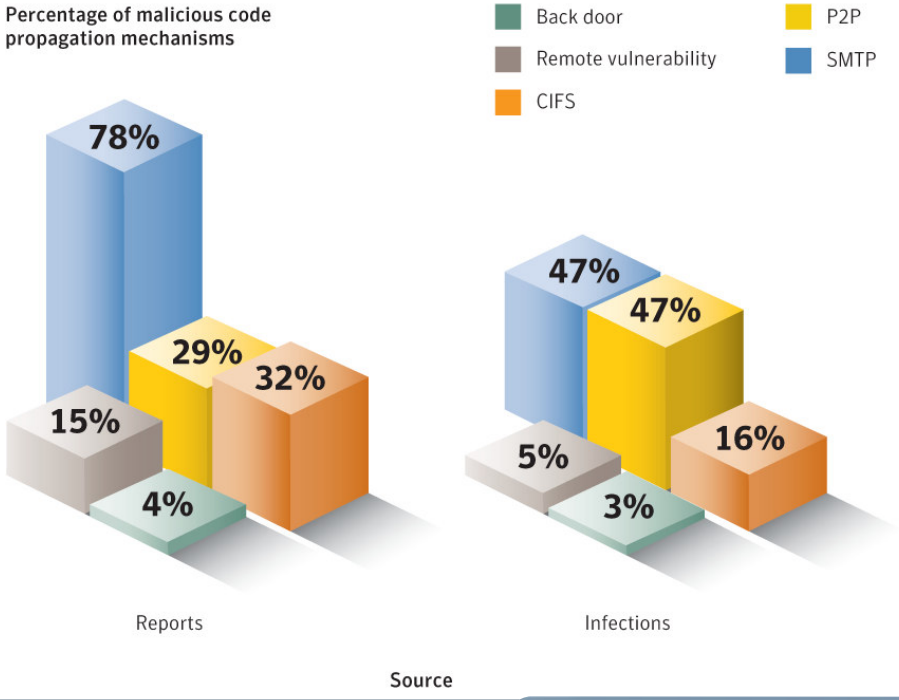
Malicious Code Trends
Threats to Confidential Information

- During the current reporting period, threats to confidential information made up 66% of the volume of top 50 malicious code reported to Symantec, up from 48% in the previous reporting period.
- While the volume of threats that allow remote access have decreased from the same reporting period last year, the volume of threats that log keystrokes and export user and system data have all increased. Keystroke loggers represent 70% of the report threats to confidential informat



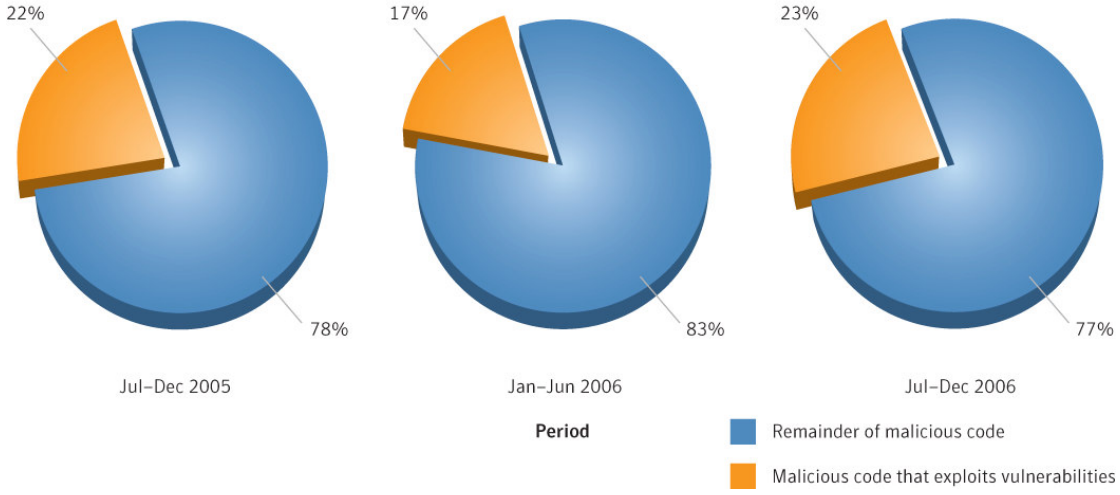
Malicious Code Trend
Propagation Vectors

- SMTP propagation remains the number one propagation mechanism by volume at 78%. This is a decrease from 98% in the previous reporting period. This is due to an increase in attackers diversifying their infection attempts and a decrease in mass mailer reports.
- When compared with potential/attempted infections, SMTP and P2P account for nearly half of all propagation methods. The difference between reports and potential/attempted infections is likely due to the presence of mass mailers.



Malicious Code Trends
Vulnerability Exploitation

- 23% of the 1,318 documented malicious code instances exploited vulnerabilities. This is an increase from the 17% in the previous reporting period.
- Malicious code that exploits vulnerabilities in 3rd party applications is on the rise - five zero-day exploits were released for vulnerabilities in Microsoft Office during the current reporting period.

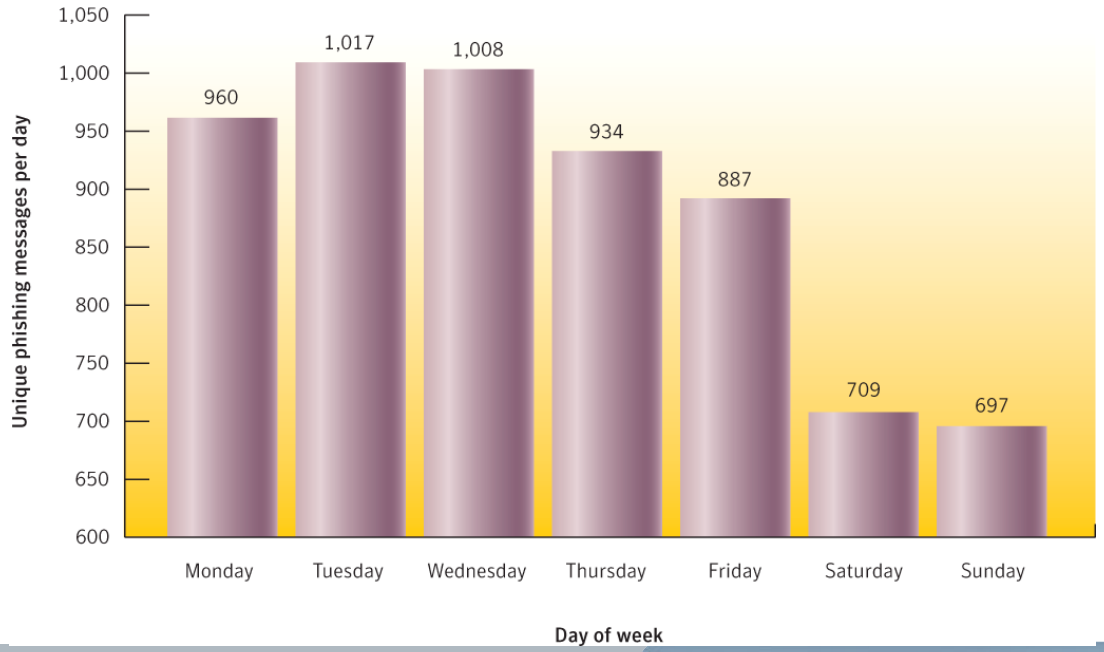


Malicious Code Trends
Additional Metrics

- Between July 1 and December 31, 2006 Symantec honeypot computers captured a total of 136 previously unseen malicious code threats up from 98 in the previous reporting period.
- 5 of the top ten new malicious code families were trojans - Stration (worm) was the number one new malicious code family reported to Symantec.
- During the current reporting period there was a 22% increase in the number of Win32 variants reported to Symantec - 8, 258.
- Polymorphic threats represent three percent of the top 50 malicious code samples reported to Symantec, up from 2% in the previous reporting period.
- The majority of malicious code reports originated in the United States.
- MSN Messenger was affected by 35% of the new instant messaging threats during the current reporting period.

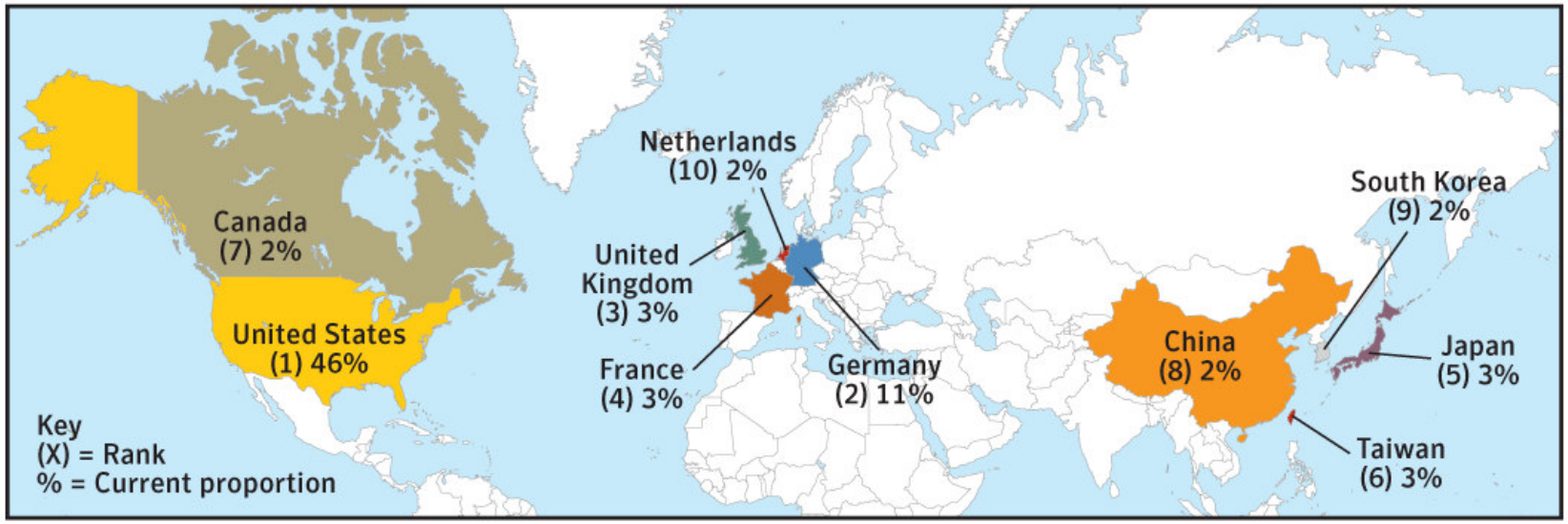
Phishing
Daily and Seasonal Variations

- Phishing activity tends to mirror an average business week as attackers attempt to mimic legitimate companies email practices. This pattern may also be due to the fact that phishing campaigns are generally short lived and are most effective when people receive and read the phishing emails soon after they were sent.
- Holidays such as Christmas and New Year and large events like the FIFA World Cup increase the amount of phishing activity. During the Christmas season, blocked phishing messages climbed to a high of 29% above the average and during the FIFA World Cup, blocked phishing attempts were 40% higher than the average.



Phishing:Top Countries Hosting Phishing Sites

- 46% of known phishing sites were located in the United States followed by Germany with 11% and the United Kingdom with 3%
- The U.S. is number one because a large number of Web-hosting providers—particularly free Web hosts— are located in the United States. Furthermore, the United States has the highest number of Internet users in the world, and it is home to a large number of Internet-connected organizations, both large and small.
- Germany has the largest number of Web-hosting providers in Europe. By hosting with large providers, phishers gain the advantage of obscurity due to the large number of sites hosted and the difficulty in tracking down a phishing site and shutting it down.



Phishing:Top Countries Hosting Phishing Sites - GCC

Top Countries for Phishing Hosts

Rank	GCC Rank	Country	Sub-region
62	**1**	United Arab Emirates	Middle-east
71	**2**	Saudi Arabia	Middle-east
82	**3**	Bahrain	Middle-east

Phishing
Additional Metrics

- The Symantec Probe network detected a total of 166,248 unique phishing messages, a six percent increase from the previous period. This translates into an average of 904 unique phishing messages per day.
- Symantec blocked over 1.5 Billion phishing messages - an increase of 19% over the first half of 2006. An average of 8.48 million per day.
- Financial services accounted for 84% of the unique brands that were phished while making up 64% of the total phishing websites. The retail sector accounted for 5% of unique brands phished and 34% of the total number of phishing websites.

Spam
Country of Origin

- 44% of all spam originated in the United States, a drop from 49% in the previous reporting period. Undetermined EU countries rank second with 7% followed by China with 6%
- Country of origin includes spam originating from spam zombies and legitimate email servers. Spam zombies are the result of an infection by a bot, worm or Trojan and show a wider distribution of spam origins.
- Distribution of Spam Zombies - U.S. 10%, China 9%, Germany 8%. 5 of the top ten spam zombie countries are in EMEA.

Country	Jul–Dec 2006	Jan–Jun 2006
United States	44%	49%
Undetermined EU Countries	7%	4%
China	6%	11%
Canada	4%	5%
United Kingdom	3%	4%
South Korea	3%	5%
Japan	3%	2%
France	3%	2%
Spain	3%	2%
Poland	3%	2%

Spam
Country of Origin – Middle East

Rank	GCC Rank	Country	Sub-region
51	**1**	United Arab Emirates	Middle-east
55	**2**	Qatar	Middle-east
64	**3**	Saudi Arabia	Middle-east
65	**4**	Kuwait	Middle-east
72	**5**	Bahrain	Middle-east
113	**6**	Yemen	Middle-east
118	**7**	Oman	Middle-east

Spam
%age of Email – Middle East

Country	GCC	Spam Percentage	Sub-region
Bahrain	**1**	85.18%	Middle-east
Kuwait	**2**	85.08%	Middle-east
Qatar	**3**	76.44%	Middle-east
United Arab Emirates	**4**	62.86%	Middle-east
Oman	**5**	62.28%	Middle-east

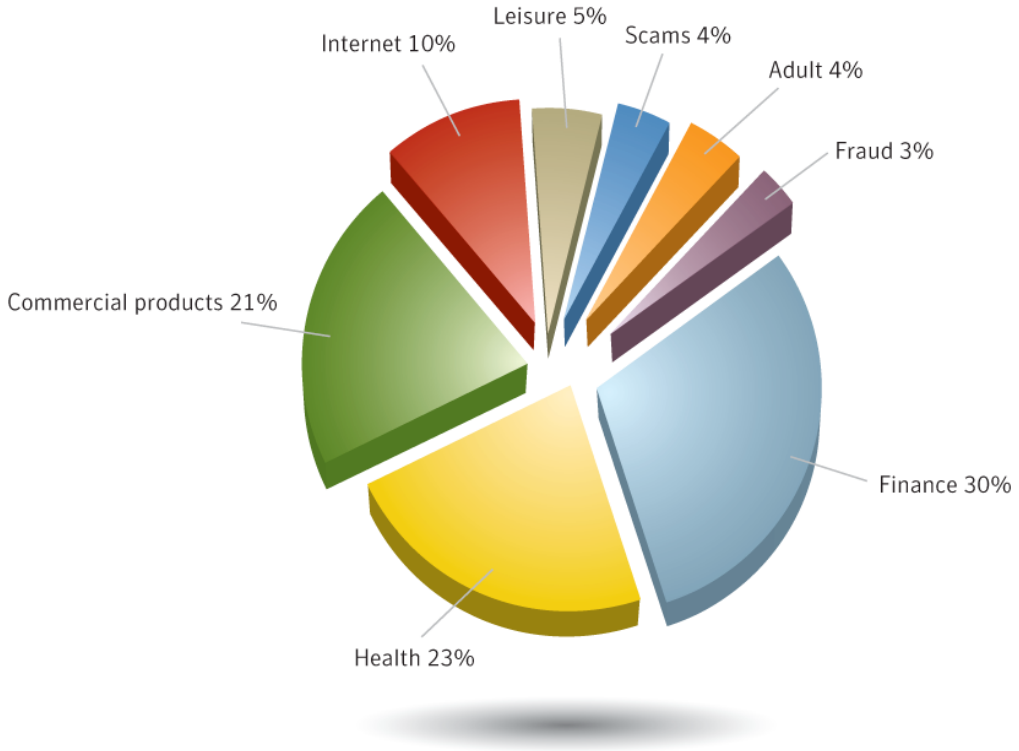
Spam Zombies – GCC

Top Countries for Spam Zombies

Rank	GCC	Country	Sub-region
71	**1**	Saudi Arabia	Middle-east
72	**2**	Kuwait	Middle-east
73	**3**	Bahrain	Middle-east
92	**4**	Qatar	Middle-east
98	**5**	United Arab Emirates	Middle-east

Spam Categories

- Spam related to Financial products or services was the top category with 30% followed by Health with 23%
- Finance grew from 15% - 30% primarily because of the rise in “pump and dump” scams and has allowed spammers to generate revenue almost immediately. Spam targeting adult products or services dropped in direct proportion to the increase in Financial spam



Spam
Additional Metrics

- Between July 1 and December 31, 2006, spam made up 59 percent of all monitored email traffic. This is an increase over the 54% in the previous reporting period.
- 65% of all spam is in English.
- During the current reporting period, 0.68% of spam contained malicious code - one out of every 147 spam messages. This is a decline from the previous reporting period where 0.81% of all spam contained malicious code.

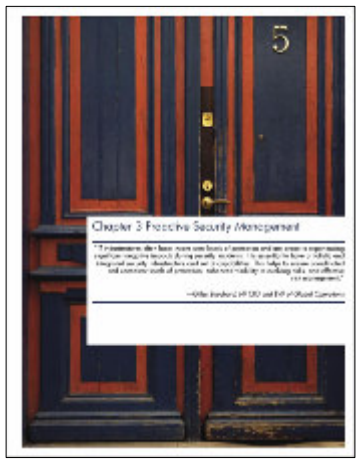
Security Risks

- Potentially unwanted applications are a new category - applications that may have an impact on security, privacy, resource consumption or are associated with other security risks.
- Movieland was the top new security risk with 41%. ZangoSearch was the top reported security risk for the current reporting period with 13%.
- Consolidation and variant-like behavior in the security risk space.

Risk Type	Percent of New Risks
Potentially unwanted applications	41%
Adware	35%
Misleading applications	18%
Dialers	0%
Security assessment tools	0%
Spyware	5%
Security risk	0%
Trackware	4%

HP Security Handbook

- Describes HP's four solution areas in detail
- Available on HP website, www.hp.com/go/security



Contact Information:

- Mahmoud Mounir, Mahmoud.Mounir@hp.com

Thank you!