



Stop Secure Threats
before they reach
YOUR BUSINESS.



Date: April 2, 2009

Nattaka K.

(nattaka@ironport.com, nkeawpra@cisco.com)

IronPort is now
part of Cisco.





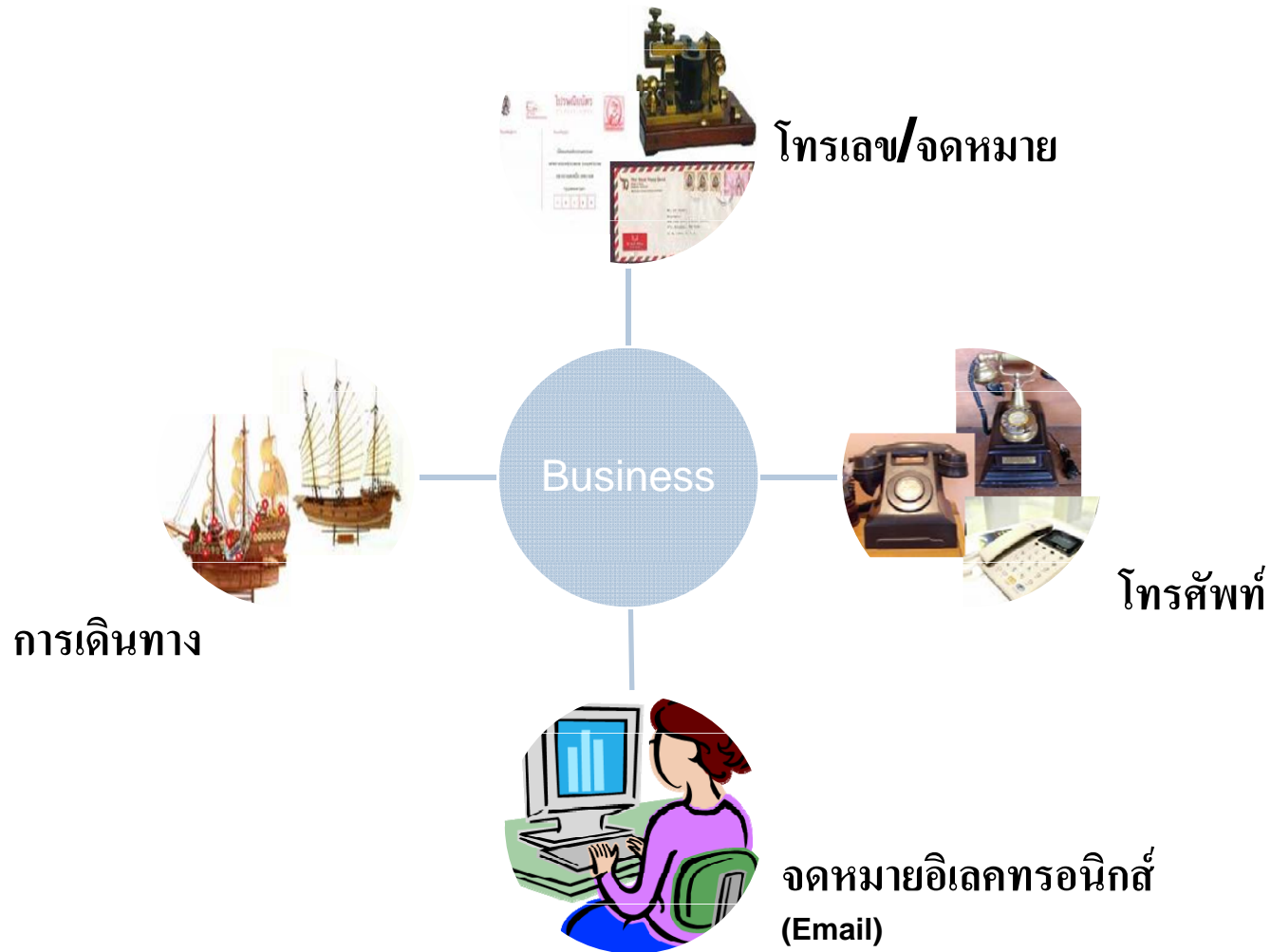
- AGENDA
 - Evolution of Business Communication
 - Spam Trends
 - Case : Banking
 - SenderBase Networks



IronPort is now
part of Cisco.



Evolution of Business Communication



SPAM Trends

Spam Mail : ถือเป็นสื่อโฆษณาที่มีต้นทุนต่ำซึ่งเปิดโอกาสให้ผู้ประกอบการธุรกิจรายใหม่ได้ ใช้ประโยชน์ในการโปรโมตสินค้าของตน แต่อย่างไรก็ตามมันก็ได้สร้างผลกระทบและความเสียหายไว้แก่ผู้รับอย่างมากไม่ว่าจะเป็นความเสียหายที่เกิดต่อผู้ให้บริการอินเทอร์เน็ตหรือ ISP ที่ระบบต้องเสียหายหรือช้าลงไปจนผิดปกติ เนื่องจากการได้รับ Spam Mail เป็นจำนวนมากจน Server ไม่สามารถรองรับได้ หรือผลกระทบที่เกิดต่อผู้รับ Spam Mail ที่ต้องเสียเวลาในการเปิดเมลล์เหล่านี้และพบว่าเป็นข้อมูลที่ไม่ต้องการ

ในปี 2003 ประเทศสหรัฐอเมริกาได้มีการออก **CAN-SPAM Act of 2003** มาควบคุม Spam Mail ซึ่งแม้จะทำให้จำนวน Spam Mail ลดลงแต่ก็ไม่สามารถจะแก้ไขปัญหาลงไปได้ เช่นเดียวกับประเทศไทยที่มีการกำหนดบทบัญญัติที่ออกมาควบคุม Spam Mail ไว้ในมาตรา 11 ของพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ระบุว่า

“ผู้ใดส่งข้อมูลคอมพิวเตอร์หรือจดหมาย อิเล็กทรอนิกส์แก่บุคคลอื่นโดยปกปิดหรือปลอมแปลงแหล่งที่มาของการส่งข้อมูล ดังกล่าว อันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข ต้องระวางโทษปรับไม่เกินหนึ่งแสนบาท”

Spam Trends

Targets of Spam – Jan 15, 2008

- Storm targets victims randomly in roughly the order you'd expect
- 1/3 spam went to top 10 domains
- Messages were addressed to 20,340 unique recipient at 8,935 domains

Top Targets of Storm Spam

Rank	Recipient domain	% Total	% Cumulative
1	hotmail.com	13.9%	13.9%
2	yahoo.com	9.3%	23.2%
3	aol.com	4.1%	27.2%
4	gmail.com	1.3%	28.6%
5	msn.com	1.0%	29.5%
6	mail.ru	0.7%	30.2%
7	sbcglobal.net	0.7%	30.9%
8	yahoo.co.in	0.6%	31.5%
9	rediffmail.com	0.5%	32.0%
10	comcast.net	0.5%	32.4%

Spam Trends

Source of Spam – Jan 15, 2008

1. By Country

- Emerging markets dominate
- Spam originated from **195** countries
- Top 10 Countries made up nearly 2/3 of spam

Rank	Country	% Storm	% Global	Difference
1	US	16.9%	18.5%	-1.5%
2	India	13.7%	2.1%	11.5%
3	Thailand	6.4%	1.3%	5.1%
4	Turkey	6.3%	4.3%	2.0%
5	Russia	5.3%	6.1%	-0.8%
6	Peru	4.9%	1.3%	3.6%
7	Poland	3.3%	3.2%	0.1%
8	Korea	3.0%	2.5%	0.4%
9	Vietnam	2.7%	0.7%	2.0%
10	Brazil	2.0%	4.7%	-2.7%

2. By Network

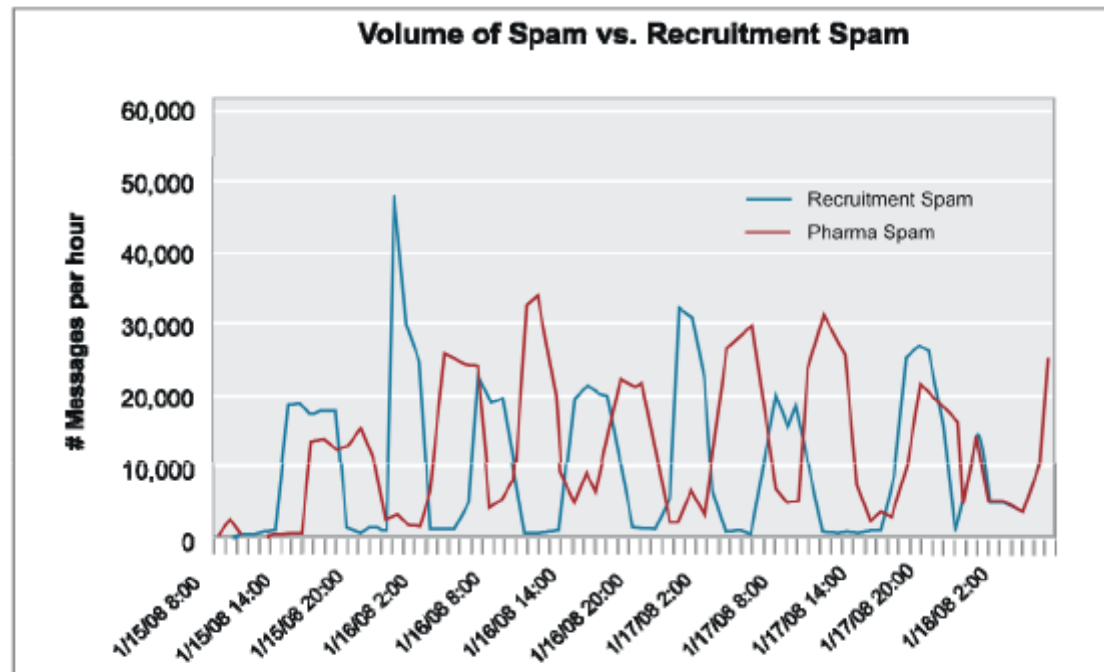
- Spam originated from **5,446** network owners
- 9 of Top 10 in emerging economies (4 from India alone)

Rank	Network owner	# IP's	% Total
1	Turk Telekom	2,450	4.6%
2	Telefonica del Peru	2,066	3.9%
3	NIB (Nat'l Internet Backbone)	1,606	3.0%
4	Videsh Sanchar Nigam Ltd	762	1.4%
5	Bharti Broadband	670	1.3%
6	True Internet Co.	650	1.2%
7	ABTS DELHI	632	1.2%
8	Neostrada Plus	432	0.8%
9	Maxnet	396	0.7%
10	Verizon Internet Services	384	0.7%
Top 10		10,048	19.0%

Spam Trends

Sending Behavior

Storm Machines Switch Between Recruit Spam and Pharma Spam



URL's rotated through 4 domains hosted on fast flux networks every 24 hours

Spam Trends

Size and Impact

- **Initial estimates of Storm's size were high and varied wildly**
 - IronPort estimated Storm sent over 20% of worldwide spam from 1.4 million IP addresses per day in July, 2007
 - Other vendors estimated the number of Storm's infected machines as high as 50 million!
- **Later estimates were lower**
 - A researcher at the University of San Diego estimated the size of Storm at between 30,000 and 40,000 peers
- **What Changed?**
 - Researchers are measuring different things
 - Storm shrank
- **We measure the impact of Storm in several ways**
 1. Storm spam volume and bots as a % worldwide spam volume
 2. The number of Storm nodes seen using P2P over time
 3. Storm population based on capture/recapture analysis of peer lists



CASE: Online Banking Useful and Harmful



IronPort is now
part of Cisco.



Bank Reputation



Bank Reputation

ระวัง!!!... phishing email SCB

posted on 03 Oct 2008 09:26 by forward-mail

ฝากเตือน คนรู้จัก ที่ใช้บริการ ธ.ไทยพาณิชย์ ด้วยนะครับ

Forward-Mail Blog :
Mail แห่งสยามประเทศ
[View my profile](#)

The Siam Commercial Bank... Bank of Choice - Windows Internet Explorer
http://209.51.132.1/~scbngro/thin/

100th Anniversary
SIAM COMMERCIAL BANK
สำหรับไทยพาณิชย์

HOME PERSONAL BANKING BUSINESS BANKING CORPORATE BANKING INVESTOR RELATIONS ABOUT SCB

PRODUCT AND SERVICES >
SERVICE CHANNELS >
RATES AND MONEY TALK >
QUICK LINK >
ONLINE BANKING
SCB EASY NET
SCB BUSINESS NET
NEW SCB BUSINESS NET
SCB FX ONLINE

Pay a bill, Win a car

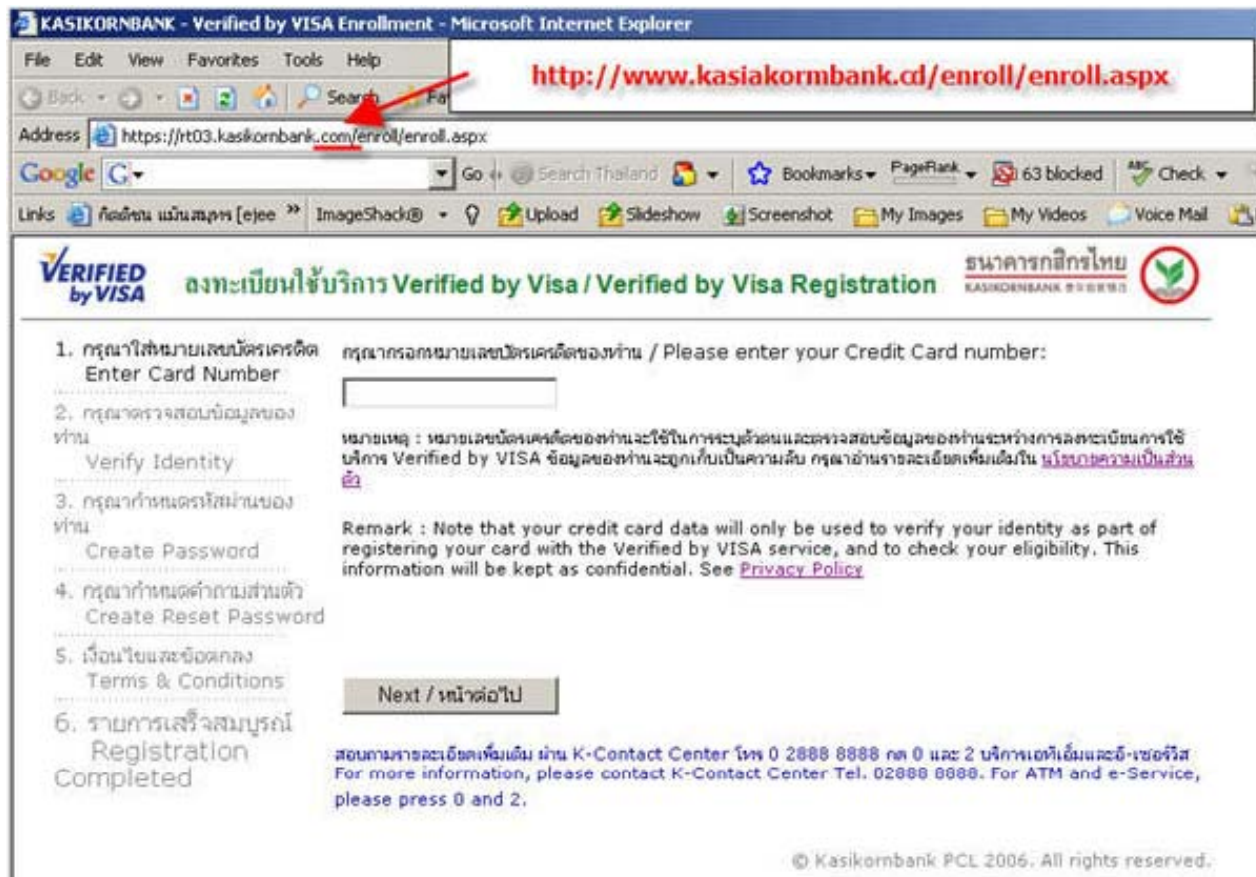
Win a Toyota Fortuner, gold, and many more prizes worth over Baht 3,500,000 in total!

Customer ID
Pin Code

- Siam bank will never ask you for your memorable data or password in an email. Never disclose this information to anyone.
- For security reasons, when



Bank Reputation



*** จากภาพ เป็น **WebPage** การสมัครใช้งาน ระบบ **Verify by Visa** ของธนาคารกสิกรไทย แต่ **Phisher** ตั้ง **Phishing Server** ใหม่เป็น <http://www.kasikornbank.cd/enroll/enroll.aspx> แทน ซึ่งหากเหยื่อไม่ทันได้สังเกต และป้อน เลขที่บัตรเครดิต ก็จบข่าว***



Bank Reputation

View Full Version : [มาแล้ว Phishing web ธนาคารกรุงเทพ ระวังให้ดี](#)

sithiphong

ข่าวด่วนร้อนฉ่ำ

ผมได้รับเมลล์จากเพื่อนแจ้งมาเ

<http://www.bangkokbank.com/Bangkok+Bank+Thai/main.htm>

มาแล้ว Phishing web ธนาคารกรุงเทพ ระวังให้ดี
www.bangkokbank.com (http://www.bangkokbank.com/) (http://www.bangkokbank.com/Bangkok+Bank+Thai/main.htm) ของปลอมนะ
http://www.palungjit.com/board/attachment.php?attachmentid=181805&stc=1&d=1182342487

ของจริงต้อง www.bbl.co.th (http://www.bbl.co.th/) (http://www.bbl.co.th/Bangkok+Bank+Thai/main.htm) ดูได้ด้านล่าง เหมือนตะ

เข้าไปดูมาแล้ว เหมือนจริงๆ ระวังกันไว้นะครับ

<!-- / message --><!-- attachments -->





The IronPort SenderBase Network



IronPort is now
part of Cisco.



The IronPort SenderBase[®] Network

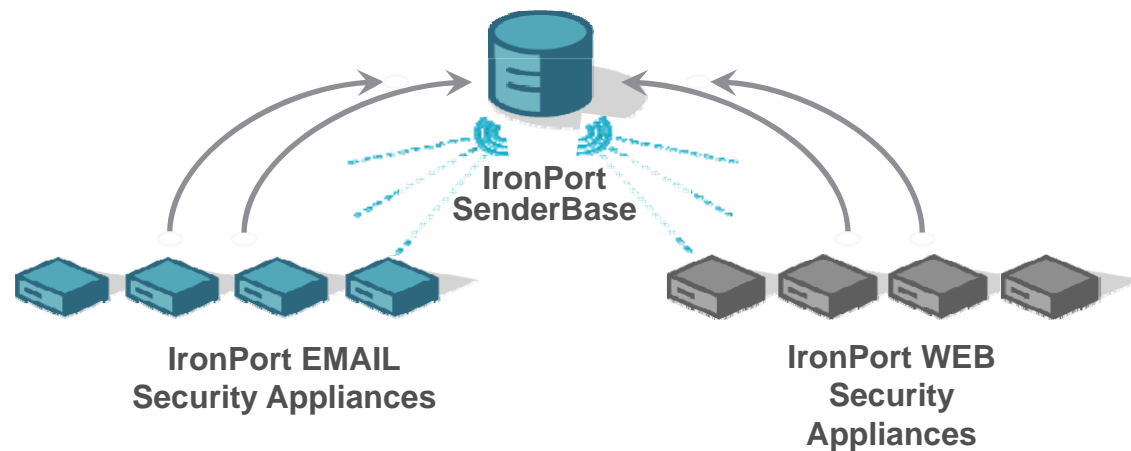
Global Reach Yields Benchmark Accuracy



- 30B+ queries daily
- 150+ Email and Web parameters
- 30% of the World's Traffic
- Cisco Network Devices

Combines Email & Web Traffic Analysis

- View into **both** Email & Web traffic
- 80% of spam contains URLs
- Email is a key distribution vector for Web-based malware
- Malware is a key distribution vector for Spam zombie infections



SenderBase IronPort Security Networks

The screenshot shows the SenderBase IronPort Security Network website. The browser window title is "SenderBase® The IronPort Security Network - Windows Internet Explorer". The address bar shows "http://www.senderbase.org/". The website features the IronPort logo and the text "SENDERBASE® IRONPORT SECURITY NETWORK". A search bar is present with the prompt "Enter domain, network owner, IP address or CIDR range [?]" and a "Search" button. The navigation menu includes "HOME", "SENDERBASE QUERIES", "THREAT OPERATIONS CENTER", "SPAMCOP", and "ABOUT".

The main content area is divided into several sections:

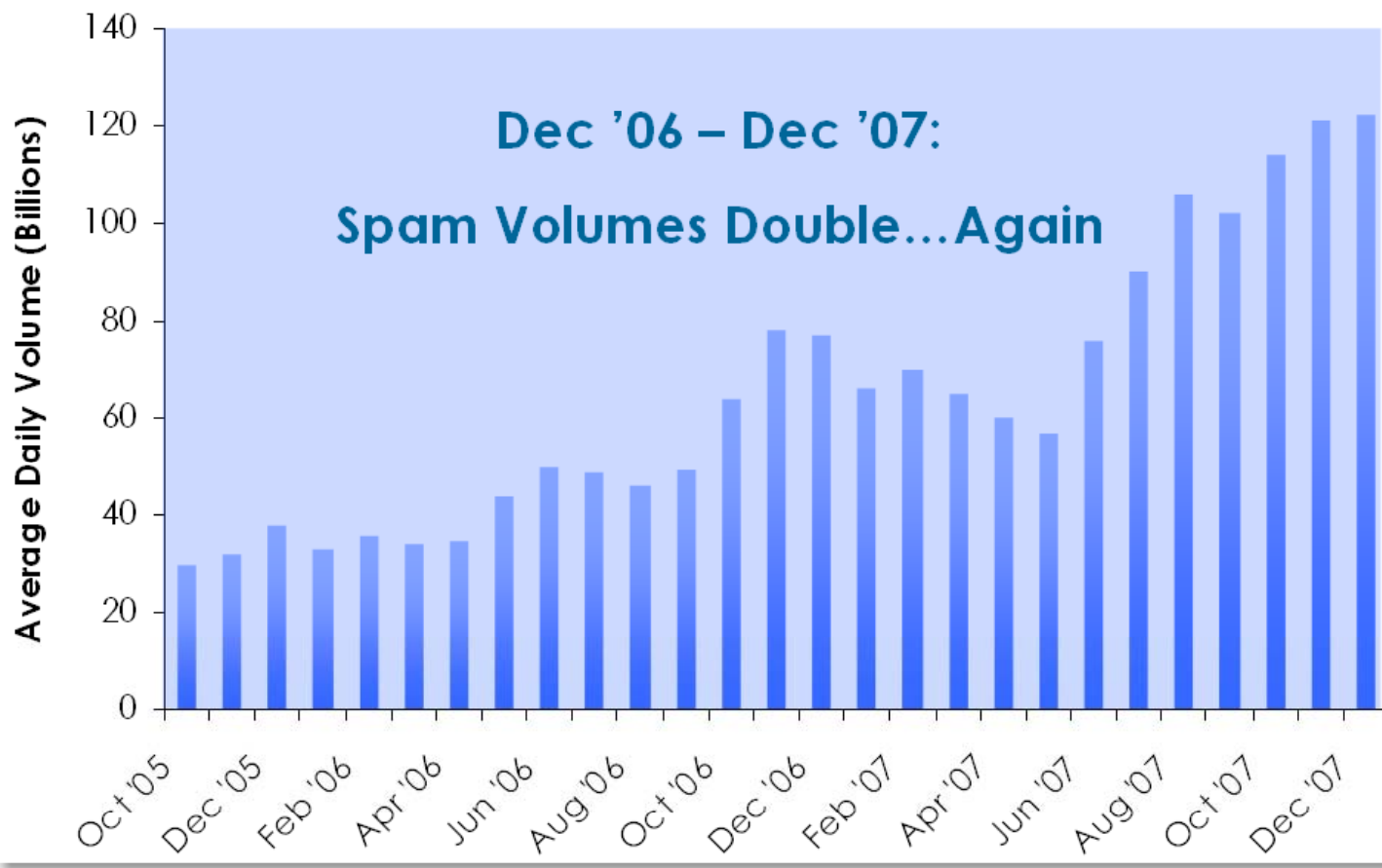
- HOME**: Summary Reports, Current Threats, Spam Watch, Virus Watch, Email & Web Reputation, Look Up, Detailed Reports, Global Email Traffic, Spam Traffic, Virus Traffic, Threat Activity Locator.
- THREAT ACTIVITY SOURCE**: A world map showing threat activity sources with markers for North America, South America, Europe, Africa, and Asia. Legend: Email Traffic (black), Spam (red), Viruses (blue).
- EMAIL & WEB REPUTATION LOOK UP**: A section with a magnifying glass icon showing a score of -6.5. Text: "You are only as credible as your online reputation. Make sure that your identity is not being compromised by criminal activity by checking your reputation score." Includes a search bar and "Search" button.
- TODAY'S GLOBAL EMAIL TRAFFIC WATCH**: A table showing email traffic data.
- CURRENT VIRUS OUTBREAK LEVEL**: A section with a "Virus Outbreak Threat Level" indicator and a "Red - Virus Outbreak In Progress" status.

IP Address	Volume (m)	Country
208.118.172.195	16.2 ↑	US
205.234.223.198	15.5 ↑	US
85.214.32.226	12.9 ↑	DE
91.147.232.194	8.7 ↑	HU

The Windows taskbar at the bottom shows the Start button, taskbar icons for Microsoft Excel, Firefox, Internet Explorer, Microsoft Office, and Norton, and the system tray with the date and time 6:12.

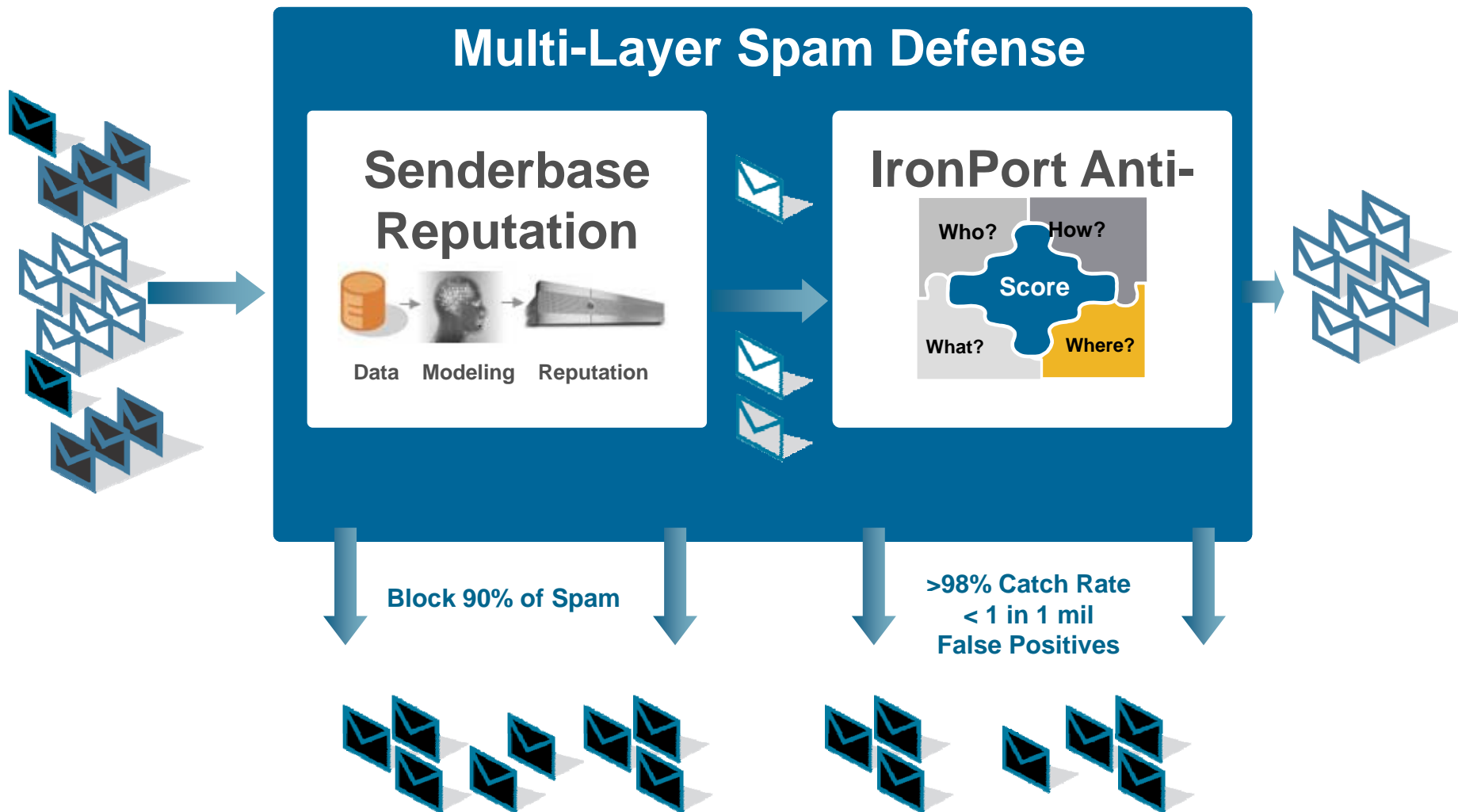
Email Trends: More Spam

Global Spam Volumes



Stop More Spam

IronPort Spam Defense



SenderBase

Reputation Filtering vs. Black Lists & White Lists

FEATURE	REPUTATION FILTERING	BLACK LISTS & WHITE LISTS
Accuracy	●	◐
Granular Scoring	●	○
Tailored Response	●	◑
Low Administrative Overhead	●	◑
Increased Message Throughput	●	◑

IronPort Spam Defense

Thompson Machinery Case Study



IronPort & Barracuda Anti-Spam Shootout Notes

	<u>IronPort</u>	<u>Barracuda</u>
Average spam received per user per day:	190	190
Spam Catch Rate:	99%	96%
Missed Spam Per Day:	18	76

Barracuda Results in 400% More Spam To The Inbox!!!

IRONPORT STOPS MORE SPAM

Thompson

“I simply plugged it in, set it up and walked away. No more spam problems! The ROI on this product is a no-brainer.”

— David Jones
IT Administrator

Thompson Machinery

MAILBOXES
PROTECTED

500+

Market Leadership

Gartner

*IronPort Positioned in the “Leaders” Quadrant
in Magic Quadrant Report*



*IronPort is positioned as a **leading player** in the
messaging security **appliance market***

THE RADICATI GROUP, INC.
A TECHNOLOGY MARKET RESEARCH FIRM

*Named IronPort the **market share leader**
in the email security appliance market*



Q&A



IronPort is now
part of Cisco.

