

FEDERAL TRADE COMMISSION

July 11-12, 2007

S **PAM**

SUMMIT

THE NEXT GENERATION OF THREATS AND SOLUTIONS

Emerging Threats

Moderator:

Sana Coleman Chriss, Attorney
and Spam Coordinator, *Division of
Marketing Practices, FTC*

Emerging Threats

- **Michael Altschul**, Senior Vice President and General Counsel, CTIA-The Wireless Association
- **Dave Champine**, Senior Director, Product Marketing, Cloudmark, Inc.
- **Scott Chasin**, Chief Technology Officer, MX Logic
- **Rick Lane**, Vice President Government Affairs, News Corporation
- **Christopher J. Rouland**, Chief Technology Officer, IBM Distinguished Engineer, IBM Internet Security Systems

Michael Altschul

- Senior Vice President and General Counsel, *CTIA - The Wireless Association*

FTC SPAM SUMMIT

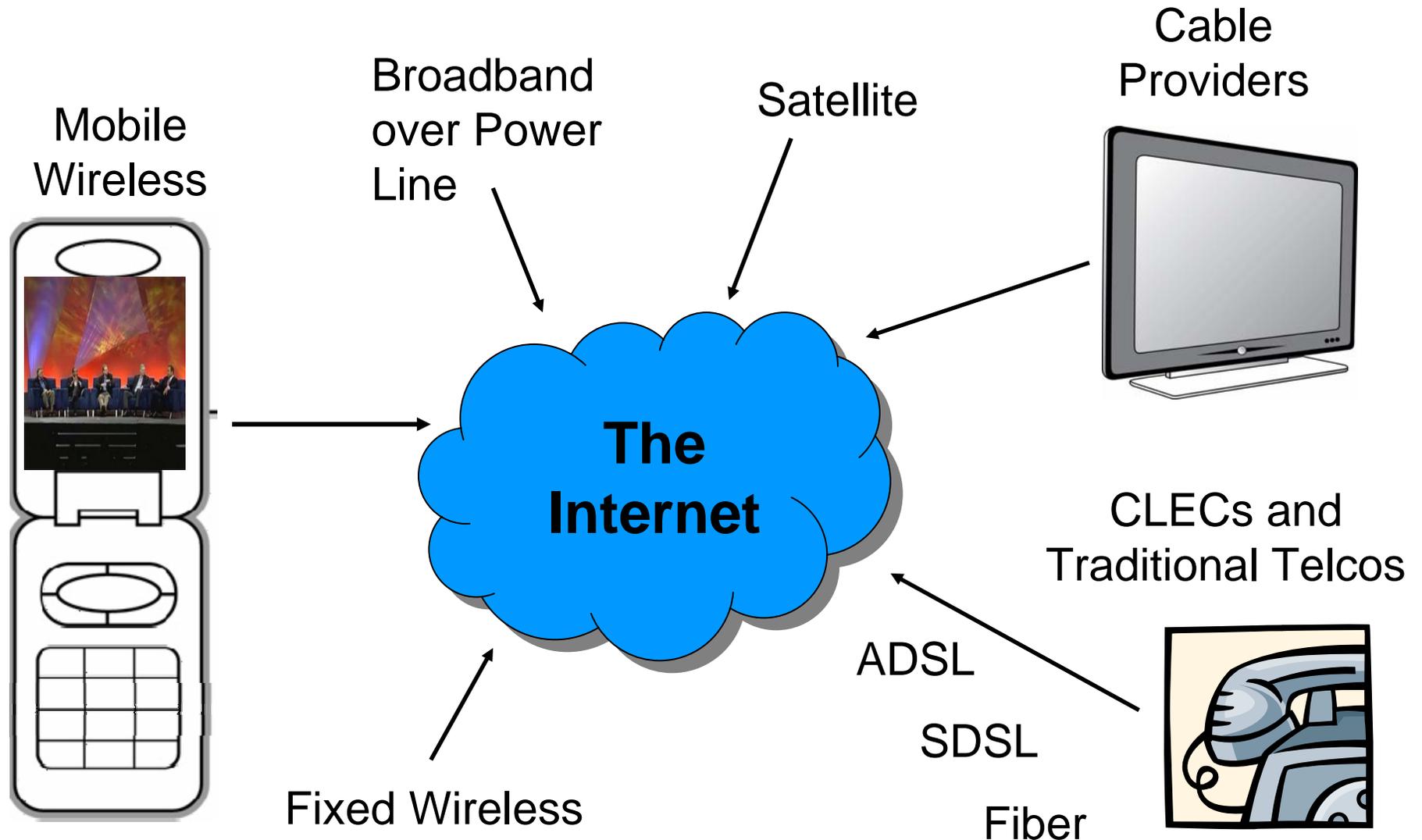
The Next Generation of Threats and Solutions

The Emerging Role of Wireless

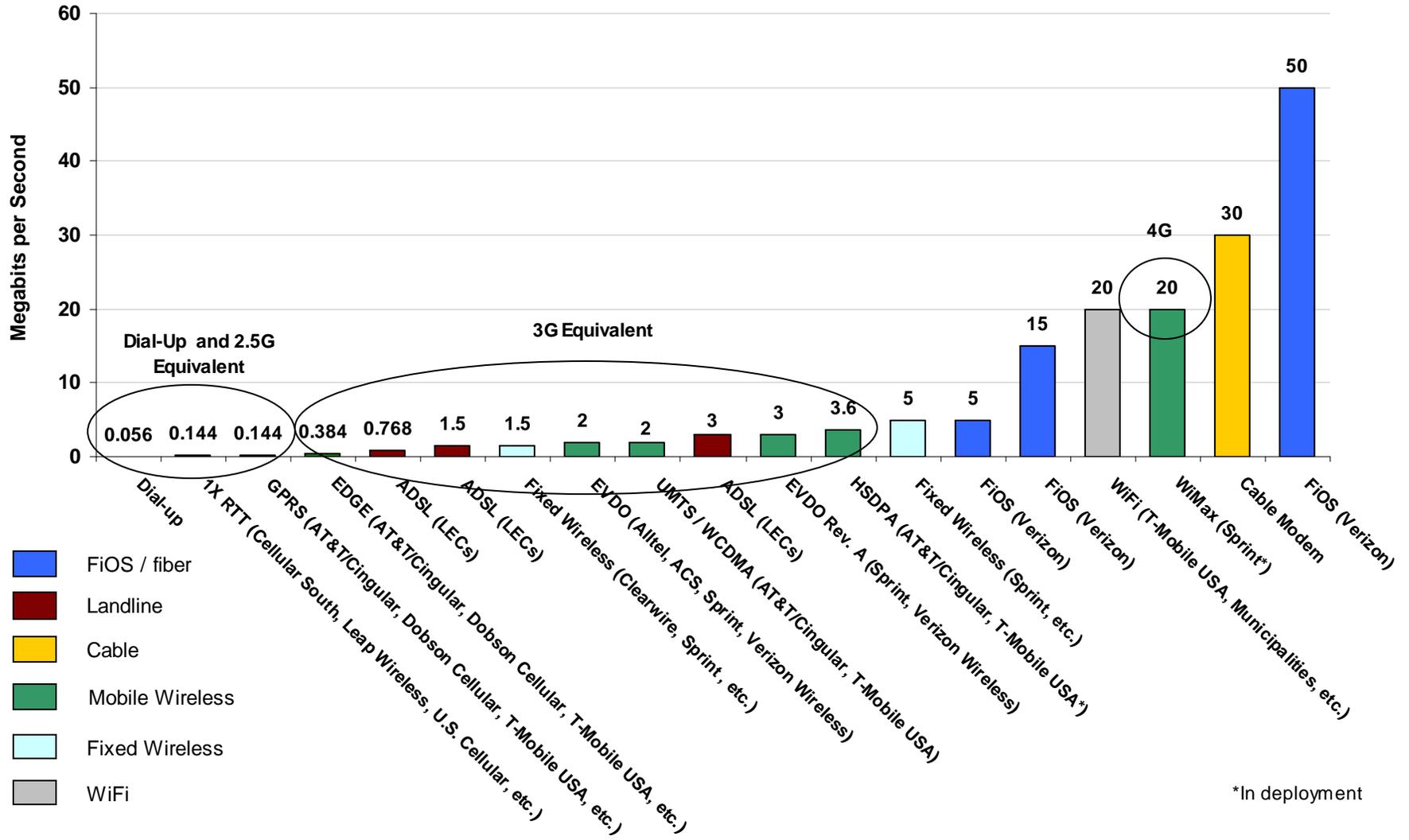
July 11, 2007

CTIA-The Wireless Association®

Multiple broadband providers and technologies access the Internet cloud



Maximum Theoretical Broadband Download Speeds



Multiple Sources: Webopedia, bandwidthplace.com, PC Magazine, service providers, ISPs, Phonescoop.com, etc.

Globally, more than 200 Mobile Broadband Devices have been Introduced



Dell Latitude
D620 / D820
Embedded **EV-DO**



Lenovo
Thinkpad
T60 / Z60
Embedded **EV-DO**



Fujitsu Lifebook Q2010
Embedded **HSDPA**



HP Compaq
nc6140 -6320
Embedded **EV-DO**

In 2006, there are more than **50** solutions available for embedded laptops or PC Cards



Franklin Wireless
CDU-550
USB Modem
21 grams, **EV-DO**



LG CU500
HSDPA, Bluetooth



Motorola Q
Windows Mobile 5
Smartphone Edition
EV-DO



Samsung SGH-ZV50
2 MP camera, AAC/MP3,
HSDPA



Casio W21CA
2.6 inch WQVGA,
2 MP Camera,
EV-DO



Novatel Wireless
Merlin S720
EV-DO Rev. A



ZTE MF330
WCDMA / **HSDPA**

More than 200 EV-DO and HSDPA devices have been commercially introduced, including PC Cards, notebooks with embedded modems, USB modems, smartphones and feature phones. Source: 3Gtoday.com

CMRS Handsets with Web Browsers

- AT&T 8525
- BlackBerry® 7130e
- BlackBerry® 8703e™
- BlackBerry® 8830
- Helio Drift
- Helio Heat
- Helio Ocean
- MOTOKRZR K1m by Motorola®
- MOTORAZR V3m by Motorola®
- MOTO Q™ by Motorola®
- Palm® Treo™ 680
- Palm® Treo™ 700p
- Palm® Treo™ 700wx
- Palm® Treo™ 750
- Samsung M510
- Samsung A727
- Samsung SCH-a990
- Verizon Wireless PN-820

CMRS Handsets with Integrated WiFi Capability

- Apple iPhone from AT&T



- T-Mobile Dash™



- AT&T 8525



- T-Mobile Wing™



- HTC Mogul™ (offered by Sprint)

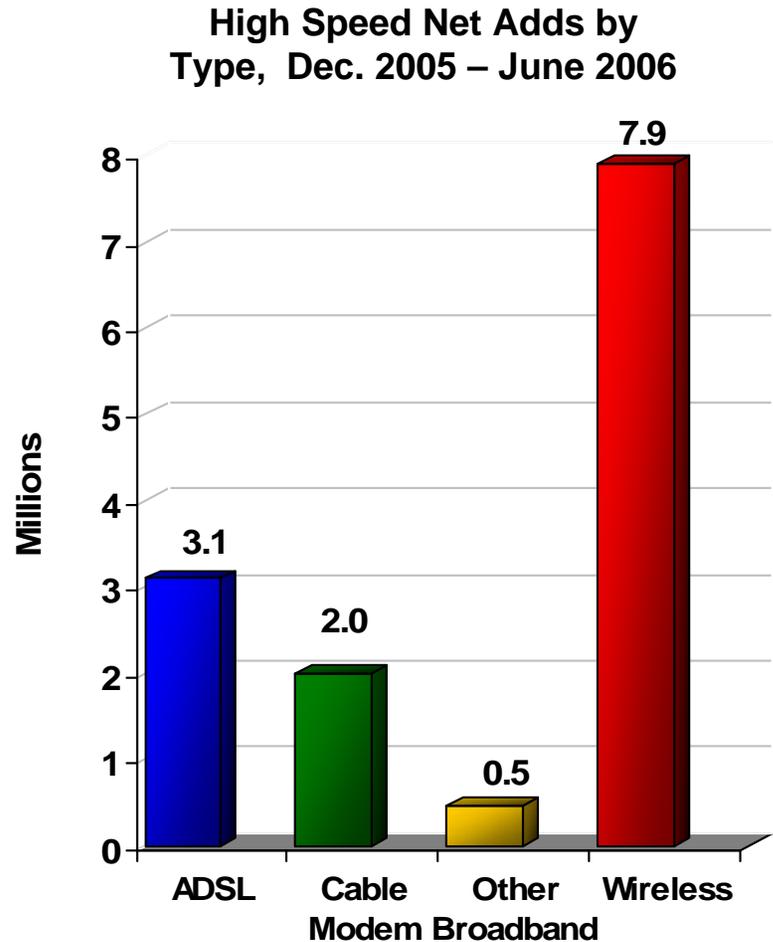


- UTStarcom 6700 (offered by Alltel, Sprint, and Verizon Wireless)



High-Speed Line Growth

- In 1H06, total high-speed lines grew 26%, from 51.2 million to 64.6 million lines, and 59% of all adds were mobile wireless subscriptions.
- From June 2005 to June 2006:
 - ADSL’s share of total broadband lines fell from 38% to 35%,
 - Cable modem’s share fell from 56% to 44%.
 - Mobile wireless’ share of total broadband lines rose from 1% to 17% of total broadband lines.
 - The share of “other” forms of broadband (including fixed wireless, satellite, fiber, and broadband over power line) remained at 4% of total broadband lines – although their total line count grew 39%.



Sources: FCC Report on “High-Speed Services for Internet Access,” Jan. 2007.

Emerging Threats

- **Michael Altschul**, Senior Vice President and General Counsel, CTIA-The Wireless Association
- **Dave Champine**, Senior Director, Product Marketing, Cloudmark, Inc.
- **Scott Chasin**, Chief Technology Officer, MX Logic
- **Rick Lane**, Vice President Government Affairs, News Corporation
- **Christopher J. Rouland**, Chief Technology Officer, IBM Distinguished Engineer, IBM Internet Security Systems

Dave Champine

- Senior Director, Product Marketing,
Cloudmark, Inc.



CLOUDMARK®

Spam is a Nasty Business

Economics 101

- Successful entrepreneurs look for large, growing markets with low-cost manufacturing and distribution
- When markets become saturated by competitors and restricted or taxed by regulators then they must seek out new markets
- Spammers are driven by the same profit motives
- Understanding their motives helps to explain current behavior and hopefully predict future trends

New Products

■ Image spam

- Elusive to most traditional techniques
- Hijacking legitimate newsletters and financial prospectus

■ Botnets

- Distributed network avoids detection
- Additional revenue opportunity from network rental
 - key loggers, spam engines, phishing hosts, etc.

■ Targeted scams

- Personalized for stronger appeal
- Social engineering is hard to protect against

New Markets

- Current Media experiencing widespread abuse in US
 - Instant Messaging
 - Blogs and RSS Feeds
 - Social Networks
- Mobile is likely to be the next major frontier
 - Unlimited text and data plans now offered by major US carriers
 - Free distribution channel
 - SMS usage increased more than 100% over last year
 - 158 billion text messages sent in 2006 by approximately 40% of users
 - Large, uneducated audience with limited solutions
 - Major investment in mobile advertising and mobile banking
 - Mobile ad spending to exceed \$10 Billion by 2010
 - High expectations with a premium on trust and security

New Challenges

■ *Wireline-to-wireless threats*

- Technology convergence is driving down the cost of bringing e-mail and web services to wireless networks
- Mobile email and internet to SMS message abuse is easily adapted from current attacks

■ *Wireless-Specific Threats*

- SMS spam
 - 18-25% of US SMS users have already received SMS spam
- “Smishing” (SMS phishing)
 - Limited screen space and unsophisticated browsers make validation difficult
- Mobile viruses and worms
 - 200 known viruses on Symbian OS
 - Bluetooth and MMS (for pictures and video) used to distribute malicious code

New Considerations

- Young people are the primary users of mobile messaging
 - Parental monitoring is much more difficult on mobile devices
 - Mobile bullying is already a major issue in the UK
- Mobile carriers have more at stake than ISPs
 - Mobile phones are considered a trusted device and a payment method
 - Carriers and businesses bear the liability for fraud
- Mobile phones lack the screen space to manage abuse
 - Technology is still developing and the variety of platforms is immense
 - Consumers focus on features first, security later

Emerging Threats

- **Michael Altschul**, Senior Vice President and General Counsel, CTIA-The Wireless Association
- **Dave Champine**, Senior Director, Product Marketing, Cloudmark, Inc.
- **Scott Chasin**, Chief Technology Officer, MX Logic
- **Rick Lane**, Vice President Government Affairs, News Corporation
- **Christopher J. Rouland**, Chief Technology Officer, IBM Distinguished Engineer, IBM Internet Security Systems

Scott Chasin

- Chief Technology Officer, *MX Logic*



The Evolution of Botnets

[Infection Vector “Push” Evolution



1. Network Services - probing for remotely exploited vulnerabilities (scanning)
2. Email - social engineering with attachment execution
3. Email - social engineering with web links
4. Email - automated malicious attachment execution on message viewing
5. Email - automated malicious binary execution embedded within trusted attachments (office files)

[Infection Vector “Pull” Evolution



- The move to pull strategies developed as a response to inbound filtering, NATs and firewalls

1. Web - disguised malicious software (unintended bundling or downloading)

2. Web - drive-by download injection using browser exploitation (javascript, iframe)

3. Web - cross-site scripting (XSS) and cross-site request forgery (CSRF)

[Push vs. Pull Botnet Evolution



- Traditional Push-based command and control botnets will become less frequent
- Inbound Command & Control communication has been historically easier to detect (especially over IRC channels) with push based bots
- Pull (or web-based) botnets are much harder to detect as C&C traffic can easily be disguised as normal web traffic
- Web 2.0 cross-site scripting and similar technologies will only fuel botnet obscurity
- Server-side malware polymorphism will also aid in stealth and C&C longevity
- The use of SSL and encryption will hamper detection effort

Emerging Threats

- **Michael Altschul**, Senior Vice President and General Counsel, CTIA-The Wireless Association
- **Dave Champine**, Senior Director, Product Marketing, Cloudmark, Inc.
- **Scott Chasin**, Chief Technology Officer, MX Logic
- **Rick Lane**, Vice President Government Affairs, News Corporation
- **Christopher J. Rouland**, Chief Technology Officer, IBM Distinguished Engineer, IBM Internet Security Systems

Rick Lane

- Vice President Government Affairs,
News Corporation



FTC Spam Summit Emerging Threats

Rick Lane

Senior Vice President Government Affairs, News Corporation

July 11, 2007

Overview

- Our approach to protect against spam
 - Technology
 - Back-end security features
 - Front-end security features
 - Partnerships
 - Working with Technology Partners
 - Working with Law Enforcement:
 - Criminal and Civil Lawsuits
 - Case Study: The Globe.com
 - Education

Technology/Security Features

- Back-End Features:
 - Phish Lock
 - Improvements to Filters
 - MySpace Links
- Front-End Features:
 - Ability to report spam
 - Flag friend requests
 - One-click to block comments

Partnerships

- Working with Technology Partners
 - Microsoft
- Working with Law Enforcement
 - MySpace's efforts in this area include:
 - Filing civil lawsuits against:
 - Sanford Wallace
 - Scott Richter
 - Securing settlements with a distributor of an authorized bot for spamming and an affiliate program for spamming
 - Criminal action against the Samy work creator

Case Study: The Globe.com

- MySpace filed a lawsuit against The Globe.com in June 2006
- The Globe.com sent almost 400,000 unsolicited email messages to MySpace users from 95 or more dummy accounts
- In the precedent setting case, the Court held The Globe.com liable for violations of three separate provisions of the federal CAN-SPAM Act, the California Business & Professions Code Section 17529.5., and for violations of MySpace's terms of use

Education

- Posting alerts for the community
- Offering members security tips:
 - Use a firewall
 - Use the latest operating system and auto-install critical updates/patches
 - Use anti-virus products
 - Use anti-spyware products

Addressing Future Threats

- Is there a need for additional legislation

Emerging Threats

- **Michael Altschul**, Senior Vice President and General Counsel, CTIA-The Wireless Association
- **Dave Champine**, Senior Director, Product Marketing, Cloudmark, Inc.
- **Scott Chasin**, Chief Technology Officer, MX Logic
- **Rick Lane**, Vice President Government Affairs, News Corporation
- **Christopher J. Rouland**, Chief Technology Officer, IBM Distinguished Engineer, IBM Internet Security Systems

Christopher J. Rouland

- Chief Technology Officer,
IBM Distinguished Engineer,
IBM Internet Security Systems



IBM Global Services

2007 FTC SPAM Summit

Emerging Threats

Chris Rouland
IBM Distinguished Engineer
CTO



IBM Internet Security Systems
Ahead of the threat.™

© Copyright IBM Corporation 2007

Does the consumer have a chance?

- **5%+ heavily traffic sites host malware or spyware (Gartner, 2007)**
- **Between 500k-700k URLs serving drive-by malware (Google, 2007)**
- **79% consumers in the US use anti-virus (Forrester, 2006)**

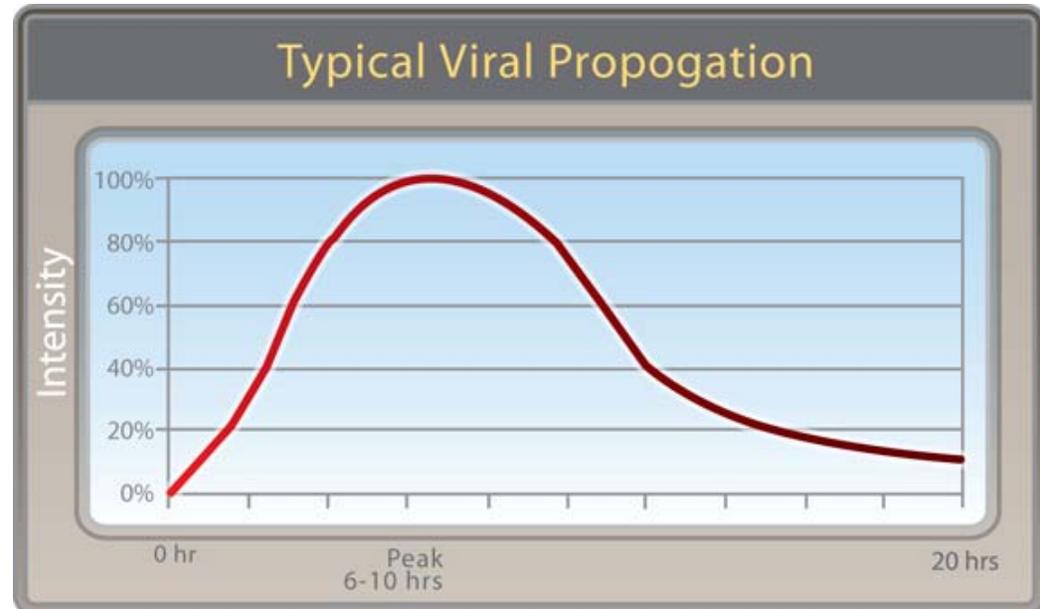


If “protection” is nearly ubiquitous, why the problem?

Malcode: Typical Attacks

Typical Attacks

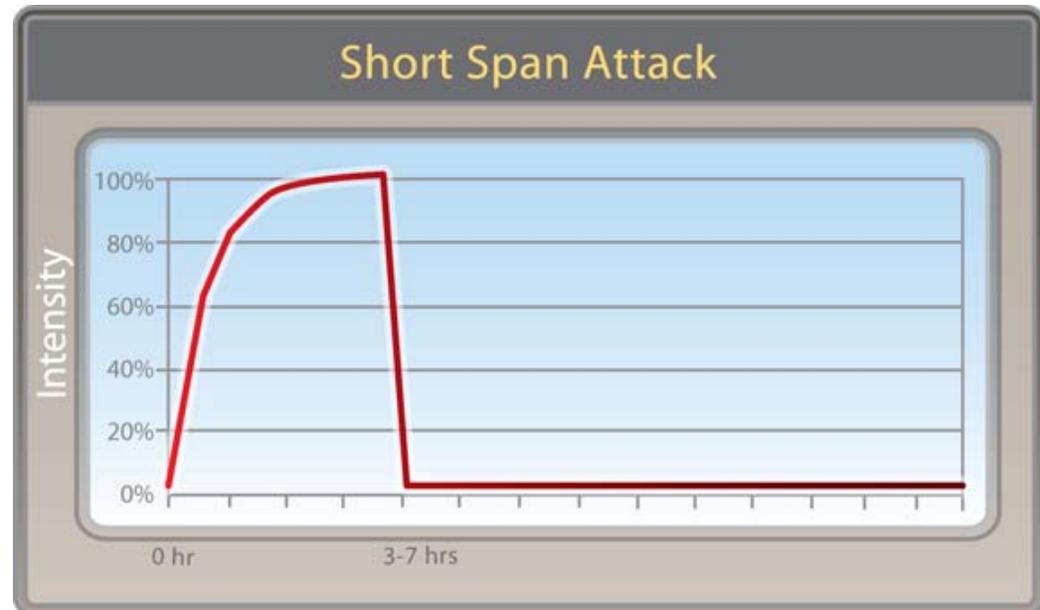
- Bell-curve shape
- Maximum intensity within a day
- Drops off after most hosts infected and difficult to find non-infected hosts



Malcode: Short-Span Attacks

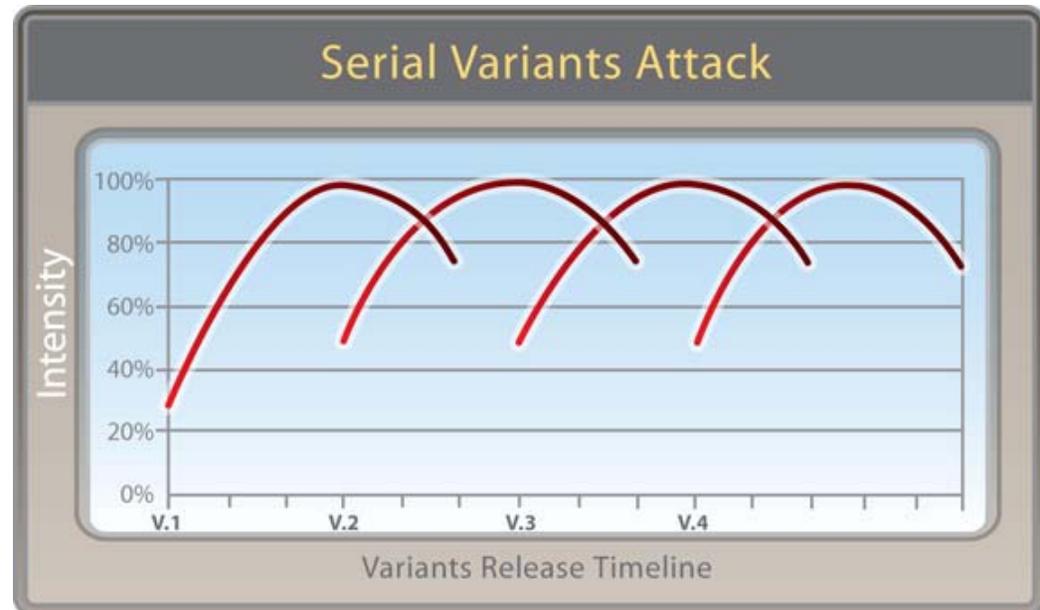
Short-Span Attacks

- Combines distribution methods of spam with worms
- Designed to infect many computers before update is available
- Entire attack is **completed in hours**



Malcode: Serial Variant Attacks

- **Serial Variant Attacks**
- **Extends window of infection**
- **Pre-Generated minor variants released at closely spaced intervals**
- **Spam Based Techniques**



2006/2007 Serial Variant Storms

Stration/Warezov Worm

Sep 24 2006	32 variants in 10 hours
Oct 1 2006	61 variants in 24 hours
Nov 6 2006	43 variants in 22 hours
Jan 14 2007	21 variants (~ 1 sample per hour)
Jan 22 2007	12 variants in 10 hours

Nuwar/Storm Worm

Jan 22 2007	30 variants in 5 hours
Feb 5 2007	27 variants in 6 hours
Feb 6 2007	11 variants in 7 hours
Feb 13 2007	55 variants in 19 hours

Emerging Threats

- **Michael Altschul**, Senior Vice President and General Counsel, CTIA-The Wireless Association
- **Dave Champine**, Senior Director, Product Marketing, Cloudmark, Inc.
- **Scott Chasin**, Chief Technology Officer, MX Logic
- **Rick Lane**, Vice President Government Affairs, News Corporation
- **Christopher J. Rouland**, Chief Technology Officer, IBM Distinguished Engineer, IBM Internet Security Systems

FEDERAL TRADE COMMISSION

July 11-12, 2007

S **PAM**

SUMMIT

THE NEXT GENERATION OF THREATS AND SOLUTIONS