Federal Trade Commission

July 11-12, 2007

Spam Summit

The Next Generation of Threats and Solutions

Evolving Methods for Sending Spam and Malware

Moderator:

Lawrence Hodapp, Attorney, *Division of Marketing Practices, FTC*

- To what extent, if any, have email address harvesting, dictionary attacks, and open proxies been replaced by botnets, zombies, and spam that uses images instead of text as the primary methods of spam distribution?

SPAM SUMMIT
July 11-12, 2007

Evolving Methods for Sending Spam and Malware

- **Ben Butler,** Director of Network Abuse, GoDaddy.com, Inc.
- **Patrick Peterson,** Vice President, Technology, IronPort Systems
- **Jon L. Praed, Esq.,** Partner, Internet Law Group
- **Suresh Ramasubramanian,** Manager, Antispam Operations, Outblaze Limited
- **Joe St Sauver, Ph.D.,** Manager, Internet2 Security Programs, Internet2 and the University of Oregon

July 11-12, 2007
SPAM SUMMIT

Patrick Peterson

- Vice President, Technology, *IronPort Systems*

Evolving Methods for Sending Spam and Malware

Only three things to remember about spammers

1. It’s about the money
2. Spam Delivery
3. Recipient Action

Spammers hostile environment stimulates constant adaptation

Spammer’s Checklist

1. Email addresses
2. Spam content
3. Spam cannons (bots)
4. Customer response infrastructure
   - Usually webserver; sometimes phone number or email address
5. Payment processing
6. Order fulfillment

The “Spam Ecosystem” section will tie it all together

1. Obtaining Email Addresses

Top three methods

1. Purchase a list of email addresses
2. Steal address book from PC via virus
3. Directory harvest attack (a.k.a. dictionary attack)
4. Harvesting from websites, IM, domain name registrations

Directory Harvest Attack

Spammer
PO Box 666
123 Spammer Ct
Kiev, Ukraine

Deborah Smith
600 Pennsylvania Avenue, N.W.,
Washington, D.C. 20580

Spammer
PO Box 666
123 Spammer Ct
Kiev, Ukraine

John Smith
600 Pennsylvania Avenue, N.W.,
Washington, D.C. 20580

Spammer
PO Box 666
123 Spammer Ct
Kiev, Ukraine

Lawrence Smith
600 Pennsylvania Avenue, N.W.,
Washington, D.C. 20580

Spammer
PO Box 666
123 Spammer Ct
Kiev, Ukraine

Deborah Jones
600 Pennsylvania Avenue, N.W.,
Washington, D.C. 20580

Spammer
PO Box 666
123 Spammer Ct
Kiev, Ukraine

Jim Smith
600 Pennsylvania Avenue, N.W.,
Washington, D.C. 20580

Spammer
PO Box 666
123 Spammer Ct
Kiev, Ukraine

Lawrence Jones
600 Pennsylvania Avenue, N.W.,
Washington, D.C. 20580

Spammer
PO Box 666
123 Spammer Ct
Kiev, Ukraine

Deborah Platt Majoras
600 Pennsylvania Avenue, N.W.,
Washington, D.C. 20580

Spammer
PO Box 666
123 Spammer Ct
Kiev, Ukraine

James Jones
600 Pennsylvania Avenue, N.W.,
Washington, D.C. 20580

Spammer
PO Box 666
123 Spammer Ct
Kiev, Ukraine

Lawrence Hodapp
600 Pennsylvania Avenue, N.W.,
Washington, D.C. 20580

Spammer’s Mail Box

Spammer
PO Box 666
123 Spammer Ct
Kiev, Ukraine

RETURN TO SENDER

Lawrence Smith
600 Pennsylvania Avenue, N.W.,
Washington, D.C. 20580

Spammer
PO Box 666
123 Spammer Ct
Kiev, Ukraine

RETURN TO SENDER

Deborah Jones
600 Pennsylvania Avenue, N.W.,
Washington, D.C. 20580

Spammer
PO Box 666
123 Spammer Ct
Kiev, Ukraine

RETURN TO SENDER

Jim Smith
600 Pennsylvania Avenue, N.W.,
Washington, D.C. 20580

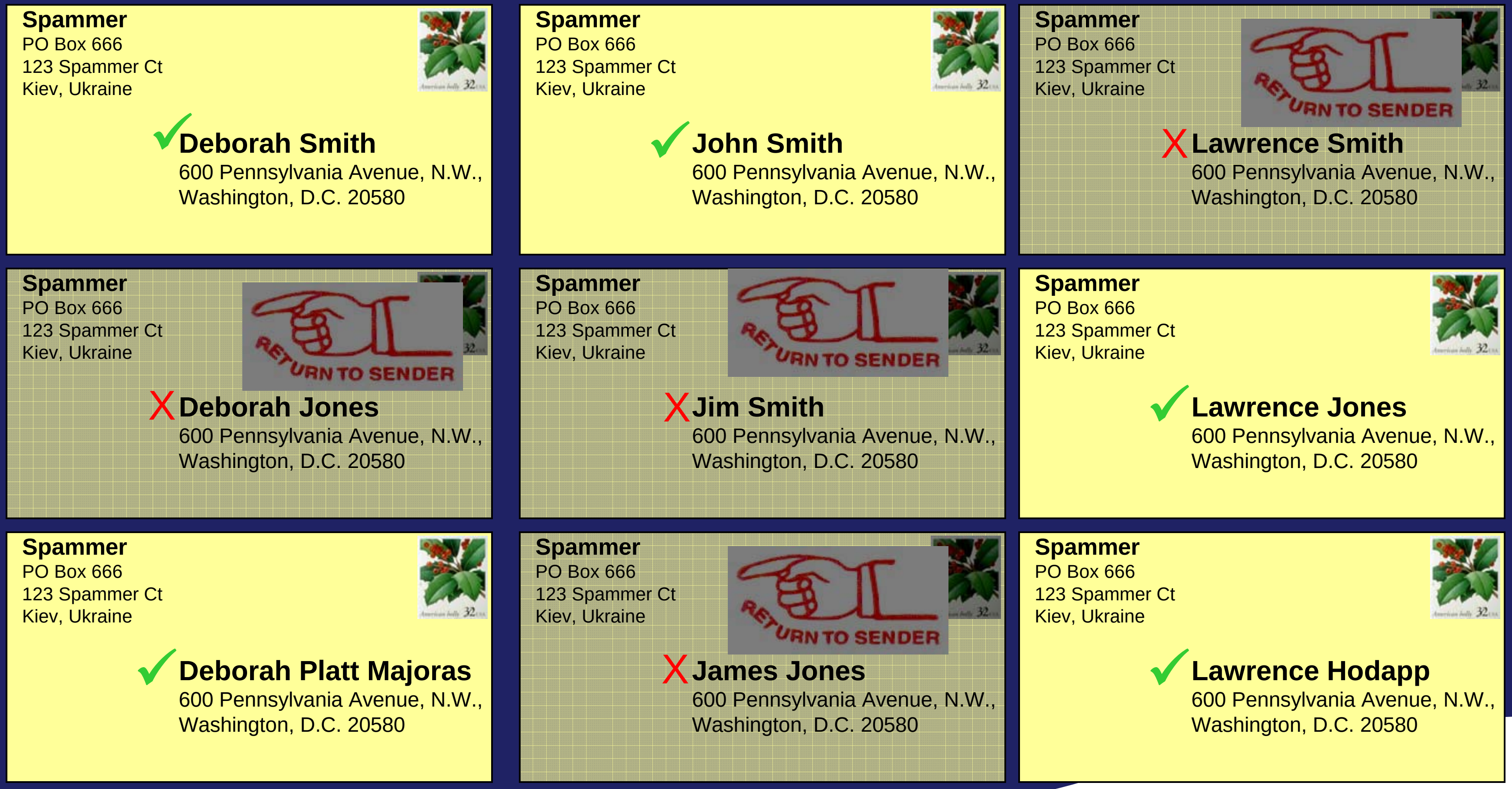
Spammer
PO Box 666
123 Spammer Ct
Kiev, Ukraine

RETURN TO SENDER

James Jones
600 Pennsylvania Avenue, N.W.,
Washington, D.C. 20580

SPAM SUMMIT
July 11-12, 2007

Directory Harvest Results



Spammer
PO Box 666
123 Spammer Ct
Kiev, Ukraine

✓ **Deborah Smith**
600 Pennsylvania Avenue, N.W.,
Washington, D.C. 20580

Spammer
PO Box 666
123 Spammer Ct
Kiev, Ukraine

✓ **John Smith**
600 Pennsylvania Avenue, N.W.,
Washington, D.C. 20580

Spammer
PO Box 666
123 Spammer Ct
Kiev, Ukraine

RETURN TO SENDER

✗ **Lawrence Smith**
600 Pennsylvania Avenue, N.W.,
Washington, D.C. 20580

Spammer
PO Box 666
123 Spammer Ct
Kiev, Ukraine

RETURN TO SENDER

✗ **Deborah Jones**
600 Pennsylvania Avenue, N.W.,
Washington, D.C. 20580

Spammer
PO Box 666
123 Spammer Ct
Kiev, Ukraine

RETURN TO SENDER

✗ **Jim Smith**
600 Pennsylvania Avenue, N.W.,
Washington, D.C. 20580

Spammer
PO Box 666
123 Spammer Ct
Kiev, Ukraine

✓ **Lawrence Jones**
600 Pennsylvania Avenue, N.W.,
Washington, D.C. 20580

Spammer
PO Box 666
123 Spammer Ct
Kiev, Ukraine

✓ **Deborah Platt Majoras**
600 Pennsylvania Avenue, N.W.,
Washington, D.C. 20580

Spammer
PO Box 666
123 Spammer Ct
Kiev, Ukraine

RETURN TO SENDER

✗ **James Jones**
600 Pennsylvania Avenue, N.W.,
Washington, D.C. 20580

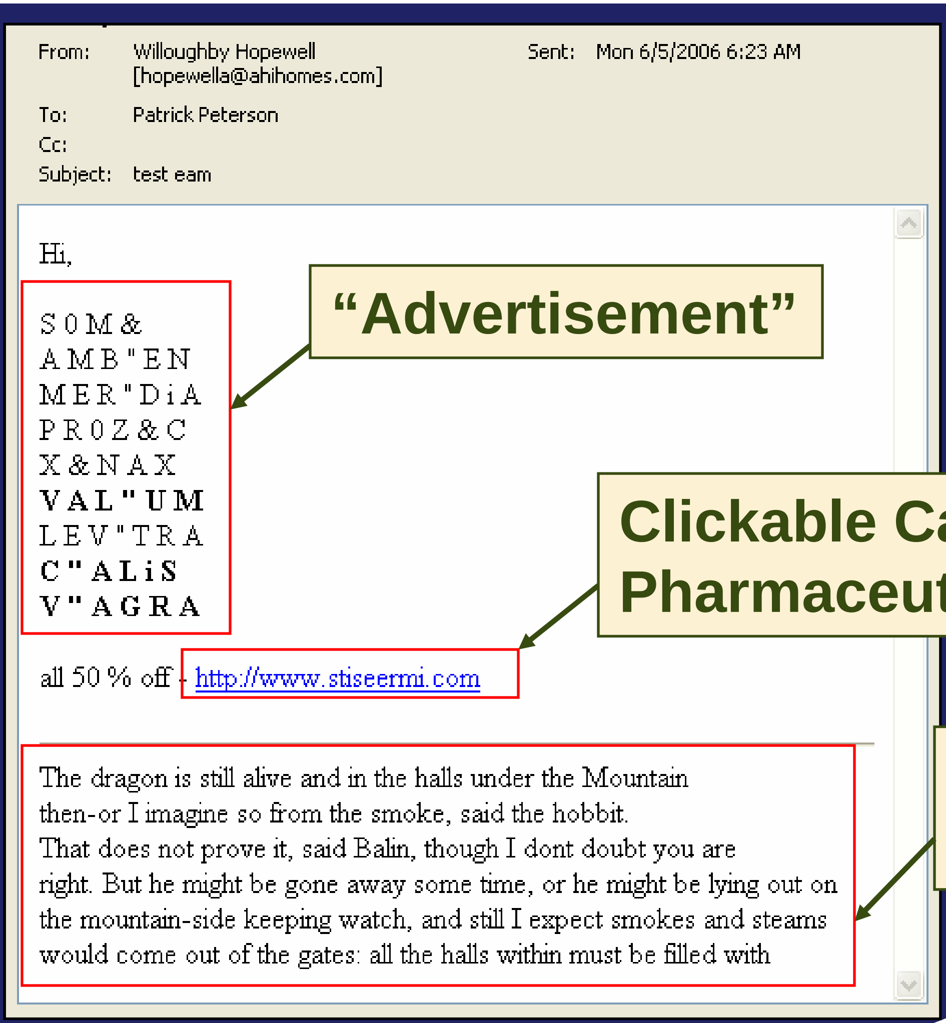
Spammer
PO Box 666
123 Spammer Ct
Kiev, Ukraine

✓ **Lawrence Hodapp**
600 Pennsylvania Avenue, N.W.,
Washington, D.C. 20580

2. Spam Content

- Remember: Delivery and Action
- Common types of spam
  - 419, Pharma/pillz, stock, mortgage, diploma, porn, “make money quick”, OEM software, gambling, mule recruitment
- Common “Call to Action” techniques
  - URL spam – user clicks on URL to visit web site
  - Image spam – call to action embedded in image, no meaningful text
  - Text spam – Spam is in plain text without image or machine-interpretable URL

Pharma: Clickable URL Spam



From: Willoughby Hopewell [hopewella@ahihomes.com]
Sent: Mon 6/5/2006 6:23 AM
To: Patrick Peterson
Cc:
Subject: test eam

Hi,

S0M&
AMB"EN
MER"DiA
PR0Z&C
X&NAX
VAL"UM
LEV"TRA
C"ALiS
V"AGRA

all 50 % off - http://www.stiseermi.com

The dragon is still alive and in the halls under the Mountain then-or I imagine so from the smoke, said the hobbit. That does not prove it, said Balin, though I dont doubt you are right. But he might be gone away some time, or he might be lying out on the mountain-side keeping watch, and still I expect smokes and steams would come out of the gates: all the halls within must be filled with

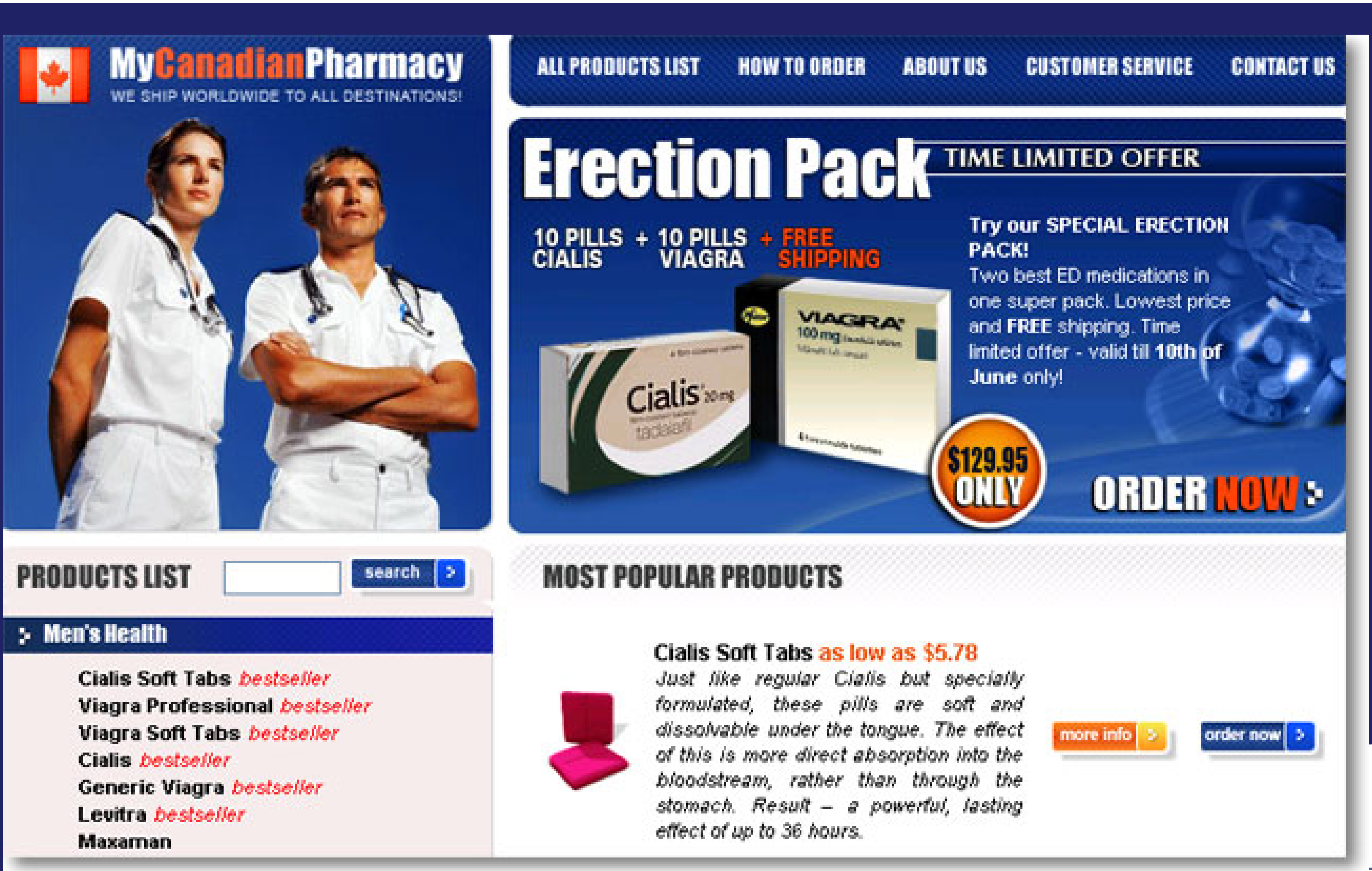
“Advertisement”

Clickable Call to Action URL Pharmaceutical Web Site

“Hashbuster” text – from “The Hobbit”

SPAM SUMMIT July 11-12, 2007

URL leads to Pharma Website



Try our SPECIAL ERECTION PACK! Two best ED medications in one super pack. Lowest price and FREE shipping. Time limited offer - valid til 10th of June only!

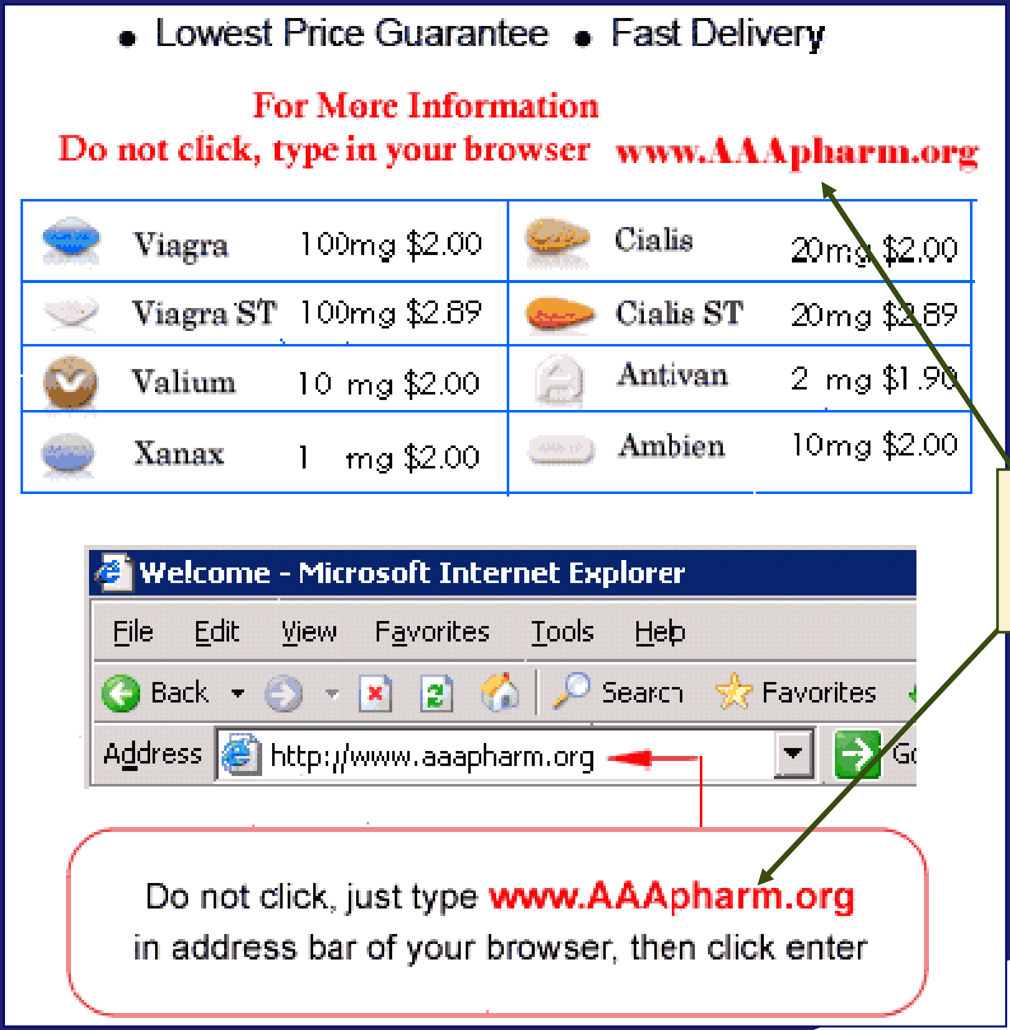
Men's Health

Cialis Soft Tabs *bestseller*
Viagra Professional *bestseller*
Viagra Soft Tabs *bestseller*
Cialis *bestseller*
Generic Viagra *bestseller*
Levitra *bestseller*
Maxaman

Cialis Soft Tabs as low as $5.78

Just like regular Cialis but specially formulated, these pills are soft and dissolvable under the tongue. The effect of this is more direct absorption into the bloodstream, rather than through the stomach. Result – a powerful, lasting effect of up to 36 hours.

Pharma: Image spam with URL



- Lowest Price Guarantee
- Fast Delivery

For More Information
Do not click, type in your browser www.AAApharm.org

Viagra	100mg $2.00		Cialis	20mg $2.00	
Viagra ST	100mg $2.89		Cialis ST	20mg $2.89	
Valium	10 mg $2.00		Antivan	2 mg $1.90	
Xanax	1 mg $2.00		Ambien	10mg $2.00	

Welcome - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Address
Go

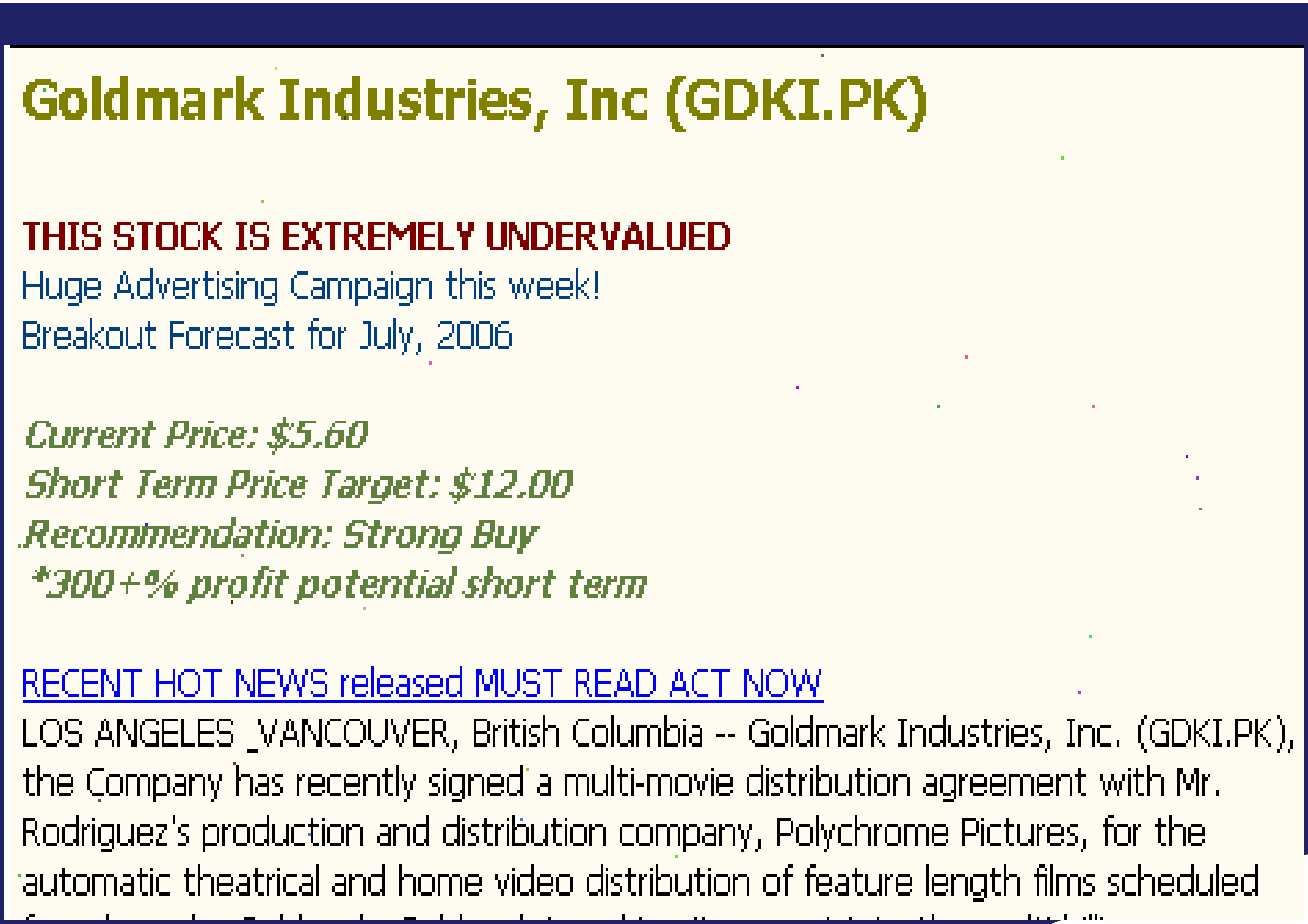
http://www.aaapharm.org

Do not click, just type www.AAApharm.org
in address bar of your browser, then click enter

URL in image, not readable by spam filters

SPAM SUMMIT July 11-12, 2007

Pump and Dump: Image Spam



Goldmark Industries, Inc (GDKI.PK)

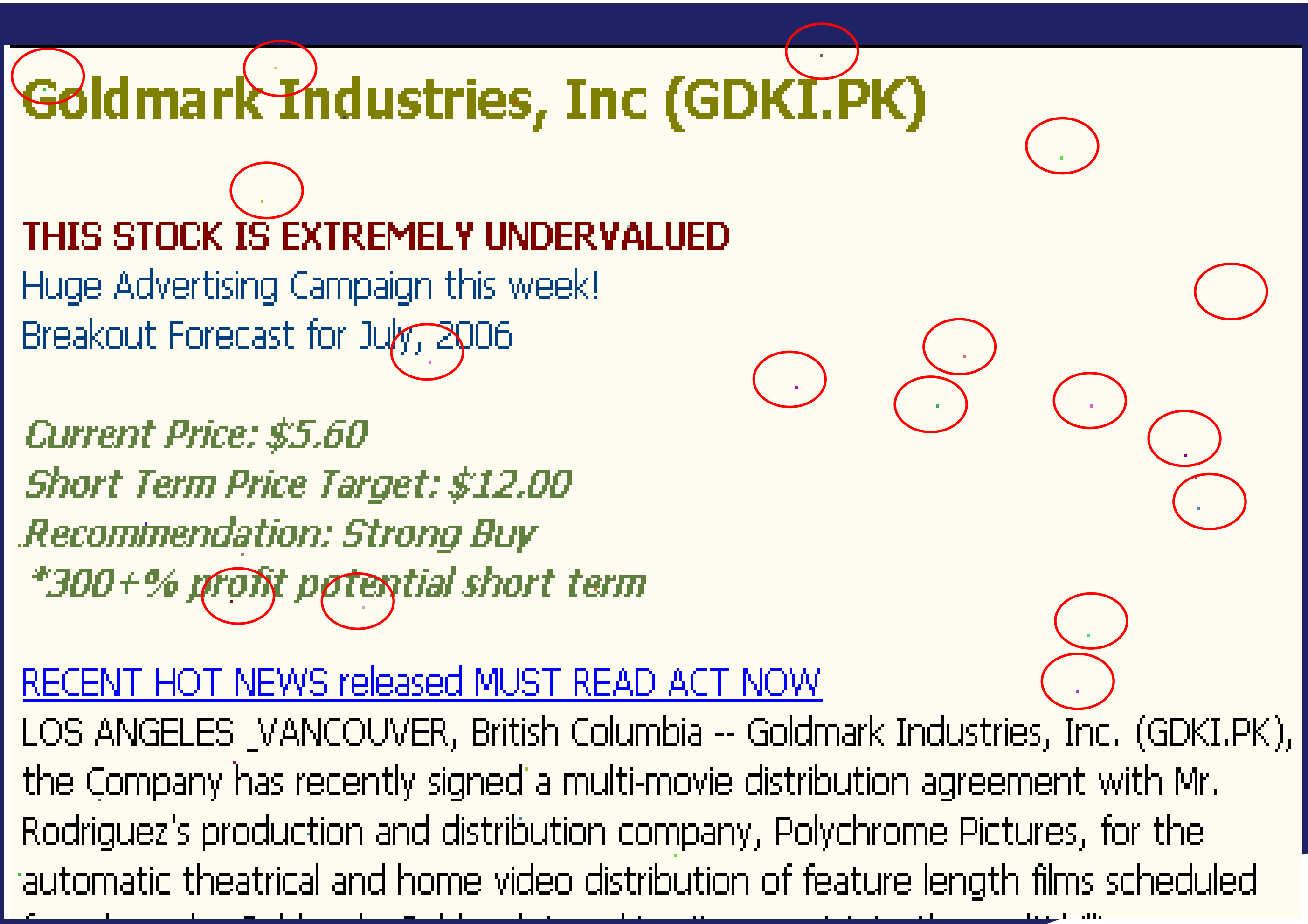
THIS STOCK IS EXTREMELY UNDERVALUED
Huge Advertising Campaign this week!
Breakout Forecast for July, 2006

Current Price: $5.60
Short Term Price Target: $12.00
Recommendation: Strong Buy
**300+% profit potential short term*

RECENT HOT NEWS released MUST READ ACT NOW

LOS ANGELES _VANCOUVER, British Columbia -- Goldmark Industries, Inc. (GDKI.PK), the Company has recently signed a multi-movie distribution agreement with Mr. Rodriguez's production and distribution company, Polychrome Pictures, for the automatic theatrical and home video distribution of feature length films scheduled

Image Spam Mutations



Goldmark Industries, Inc (GDKI.PK)

THIS STOCK IS EXTREMELY UNDERVALUED

Huge Advertising Campaign this week!

Breakout Forecast for July, 2006

Current Price: $5.60

Short Term Price Target: $12.00

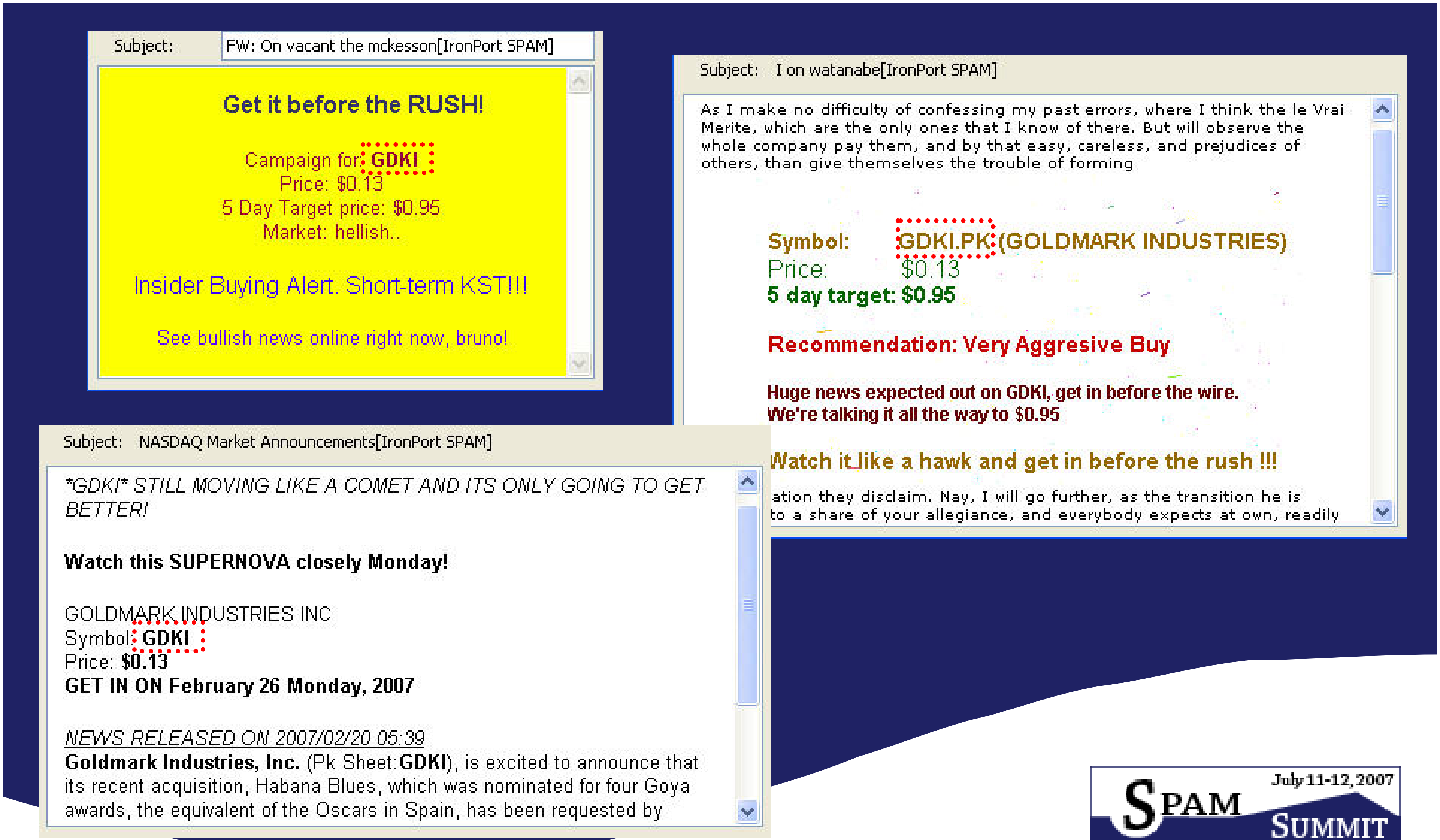
Recommendation: Strong Buy

**300+% profit potential short term*

RECENT HOT NEWS released MUST READ ACT NOW

LOS ANGELES _VANCOUVER, British Columbia -- Goldmark Industries, Inc. (GDKI.PK), the Company has recently signed a multi-movie distribution agreement with Mr. Rodriguez's production and distribution company, Polychrome Pictures, for the automatic theatrical and home video distribution of feature length films scheduled

Goldmark's Greatest Hits



Subject: FW: On vacant the mckesson[IronPort SPAM]

Get it before the RUSH!

Campaign for: GDKI
Price: $0.13
5 Day Target price: $0.95
Market: hellish..

Insider Buying Alert. Short-term KST!!!

See bullish news online right now, bruno!

Subject: I on watanabe[IronPort SPAM]

As I make no difficulty of confessing my past errors, where I think the le Vrai Merite, which are the only ones that I know of there. But will observe the whole company pay them, and by that easy, careless, and prejudices of others, than give themselves the trouble of forming

Symbol: GDKI.PK (GOLDMARK INDUSTRIES)
Price: $0.13
5 day target: $0.95

Recommendation: Very Aggresive Buy

Huge news expected out on GDKI, get in before the wire.
We're talking it all the way to $0.95

Watch it like a hawk and get in before the rush !!!

ation they disclaim. Nay, I will go further, as the transition he is to a share of your allegiance, and everybody expects at own, readily

Subject: NASDAQ Market Announcements[IronPort SPAM]

**GDKI* STILL MOVING LIKE A COMET AND ITS ONLY GOING TO GET BETTER!*

Watch this SUPERNOVA closely Monday!

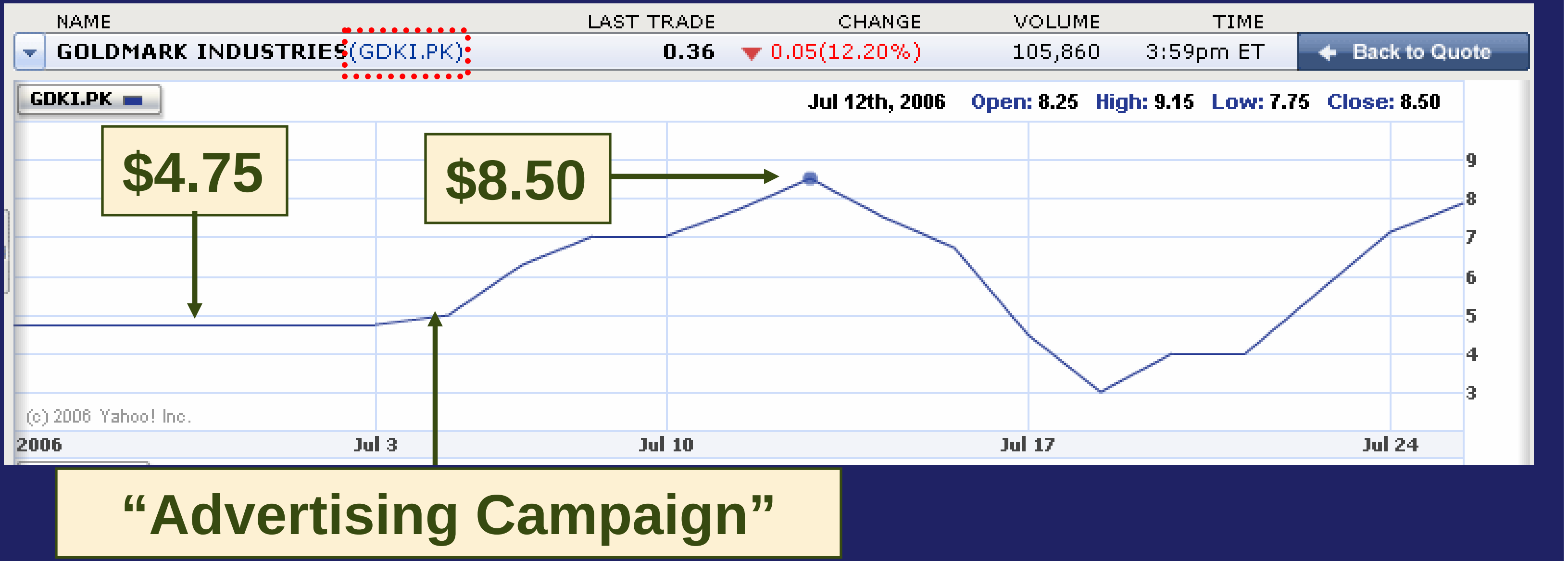
GOLDMARK INDUSTRIES INC
Symbol: **GDKI**
Price: **$0.13**
GET IN ON February 26 Monday, 2007

NEWS RELEASED ON 2007/02/20 05:39
Goldmark Industries, Inc. (Pk Sheet: **GDKI**), is excited to announce that its recent acquisition, Habana Blues, which was nominated for four Goya awards, the equivalent of the Oscars in Spain, has been requested by

SPAM SUMMIT July 11-12, 2007

Pump and Dump Works!

80% gain in six days

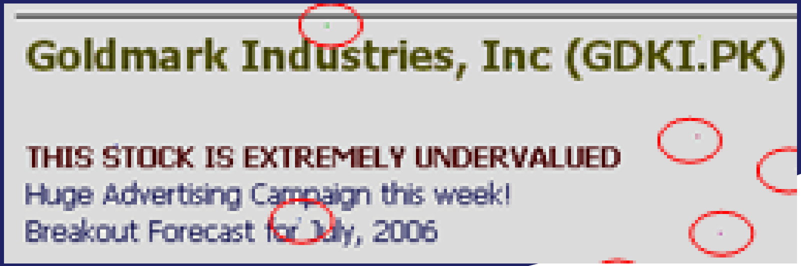


NAME	LAST TRADE	CHANGE	VOLUME	TIME	
GOLDMARK INDUSTRIES(GDKI.PK)	0.36	▼ 0.05(12.20%)	105,860	3:59pm ET	Back to Quote

$4.75

$8.50

“Advertising Campaign”



Goldmark Industries, Inc (GDKI.PK)

THIS STOCK IS EXTREMELY UNDERVALUED
Huge Advertising Campaign this week!
Breakout Forecast for July, 2006

SPAM SUMMIT July 11-12, 2007

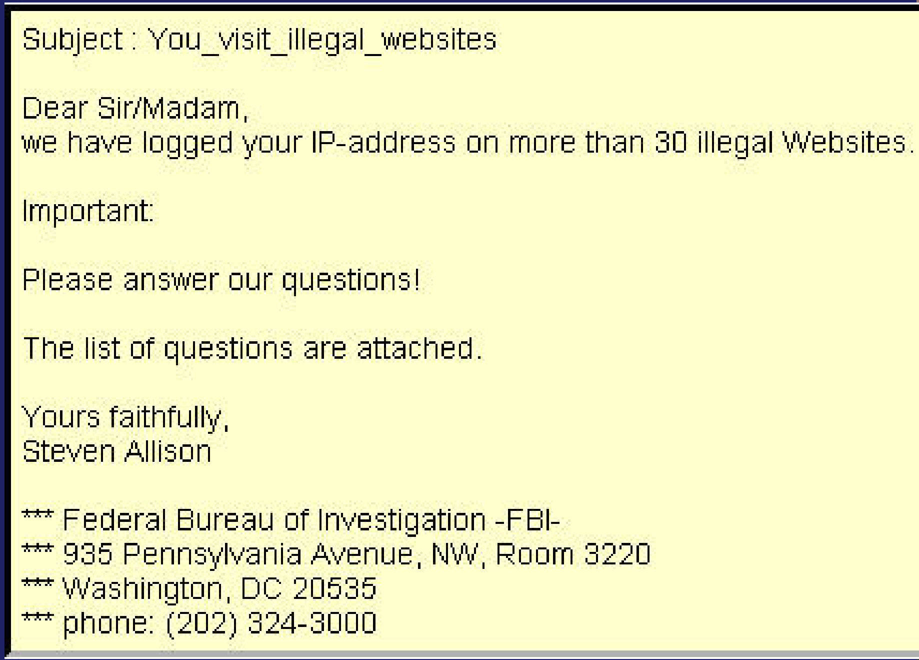
Spam Statistics

- 2006 was “The Year of Spam”
  - From 32 billion/day to 75 billion/day
  - Image spam from 5% to 30% of all spam
- 2007 holding steady at 60-70B/day
- Most email is spam
  - SenderBase.org: 90% of all email is spam
  - Messaging Anti-Abuse Working Group (MAAWG): 75% of all email is identified by ISPs as abusive
- Seeing 20,000 significant spam variants (attacks) per day

3. Spam cannons (Bots)

- Evolution from spammers’ servers to bots
- Bot Definition: PC controlled by spammer to send spam
  - Also known as Zombies
- Bots responsible for 95% of all spam
- About 10 million bots sending spam
- Bots used for many other purposes
  - Denial of Service, phishing, key logging, directory harvest, hosting content, DNS, scanning other hosts, sniffing traffic on the wire…

Creation of a bot



Subject : You_visit_illegal_websites

Dear Sir/Madam,
we have logged your IP-address on more than 30 illegal Websites.

Important:

Please answer our questions!

The list of questions are attached.

Yours faithfully,
Steven Allison

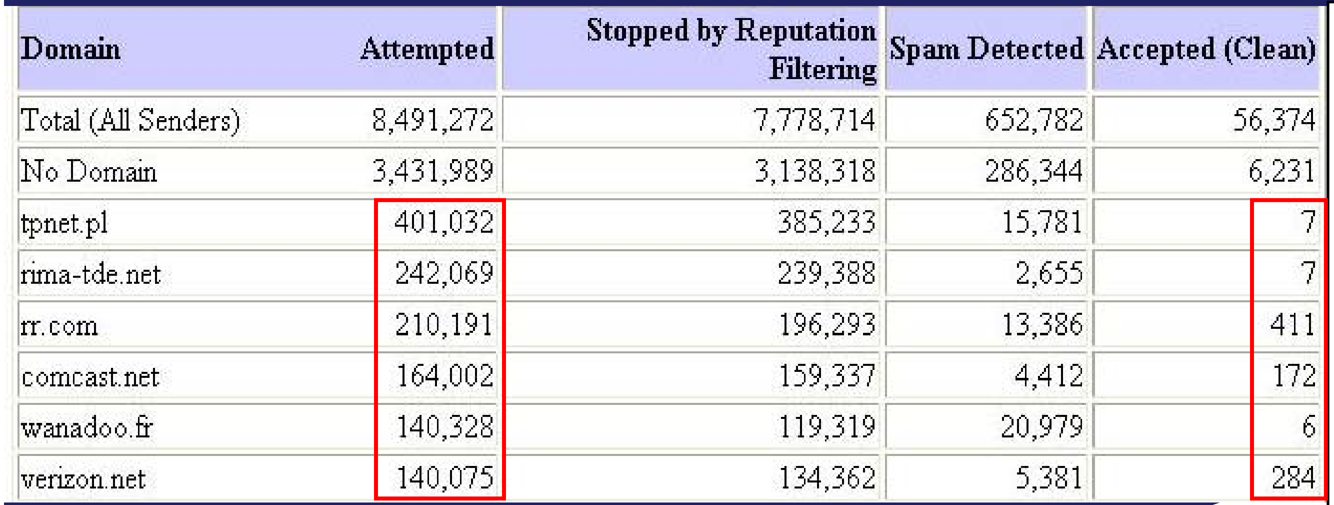
*** Federal Bureau of Investigation -FBI-
*** 935 Pennsylvania Avenue, NW, Room 3220
*** Washington, DC 20535
*** phone: (202) 324-3000

More on Bots and Spam Cannons

- Controlling millions of bots isn’t easy
- “Botnet”: Group of bots with shared “Command and Control” network
  - Sophisticated communication, e.g. P2P
- Bot University
- Panel will discuss other spam cannon devices (like web servers)

Broadband Network Bot Infestations

- Screenshot from US enterprise dashboard
- Identifies spam and legit incoming email
- Cleanest carrier: 2 in 1000 emails are legit



Domain	Attempted	Stopped by Reputation Filtering	Spam Detected	Accepted (Clean)
Total (All Senders)	8,491,272	7,778,714	652,782	56,374
No Domain	3,431,989	3,138,318	286,344	6,231
tpnet.pl	401,032	385,233	15,781	7
rima-tde.net	242,069	239,388	2,655	7
rr.com	210,191	196,293	13,386	411
comcast.net	164,002	159,337	4,412	172
wanadoo.fr	140,328	119,319	20,979	6
verizon.net	140,075	134,362	5,381	284

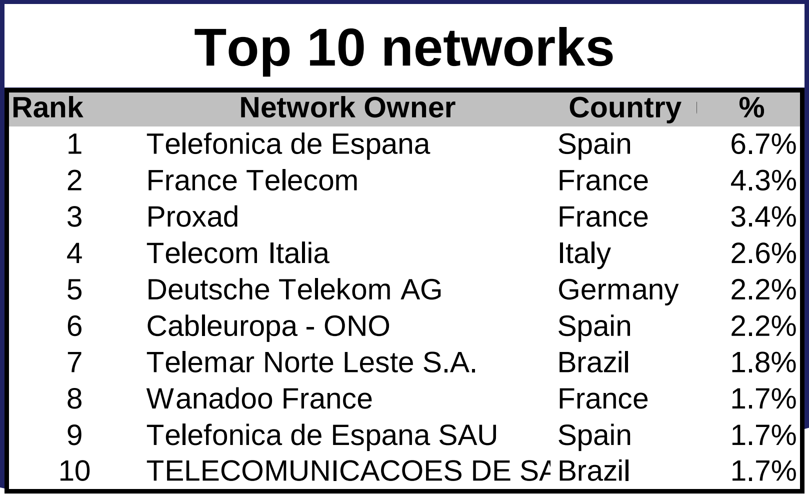
% Good	Mail Source
0.6639%	All mail
0.1816%	No rDNS
0.0017%	Polish Telecom
0.0029%	Telefonica
0.1955%	RoadRunner
0.1049%	Comcast
0.0043%	France Telecom
0.2027%	Verizon

Top email volume senders to a US enterprise

SPAM SUMMIT July 11-12, 2007

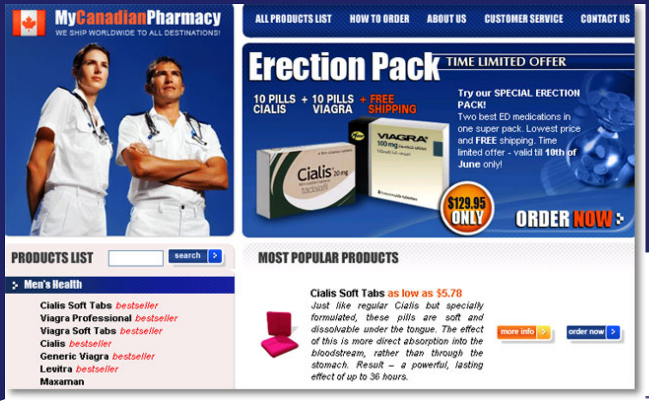
MyCanadianPharmacy Botnet

- 1.5 Billion spam/day attack
- 106,000 bots
- From 3,200 networks in 119 countries
- 25 networks sent 50% of spam



Top 10 networks

Rank	Network Owner	Country	%
1	Telefonica de Espana	Spain	6.7%
2	France Telecom	France	4.3%
3	Proxad	France	3.4%
4	Telecom Italia	Italy	2.6%
5	Deutsche Telekom AG	Germany	2.2%
6	Cableuropa - ONO	Spain	2.2%
7	Telemar Norte Leste S.A.	Brazil	1.8%
8	Wanadoo France	France	1.7%
9	Telefonica de Espana SAU	Spain	1.7%
10	TELECOMUNICACOES DE SA	Brazil	1.7%



MyCanadianPharmacy
WE SHIP WORLDWIDE TO ALL DESTINATIONS!

Erection Pack TIME LIMITED OFFER

10 PILLS CIALIS + 10 PILLS VIAGRA + FREE SHIPPING

Try our SPECIAL ERECTION PACK! Two best ED medications in one super pack. Lowest price and FREE shipping. Time limited offer - valid till 10th of June only!

$129.95 ONLY

ORDER NOW

PRODUCTS LIST

Men's Health

Cialis Soft Tabs bestseller
Viagra Professional bestseller
Viagra Soft Tabs bestseller
Cialis bestseller
Generic Viagra bestseller
Levitra bestseller
Maxaman

MOST POPULAR PRODUCTS

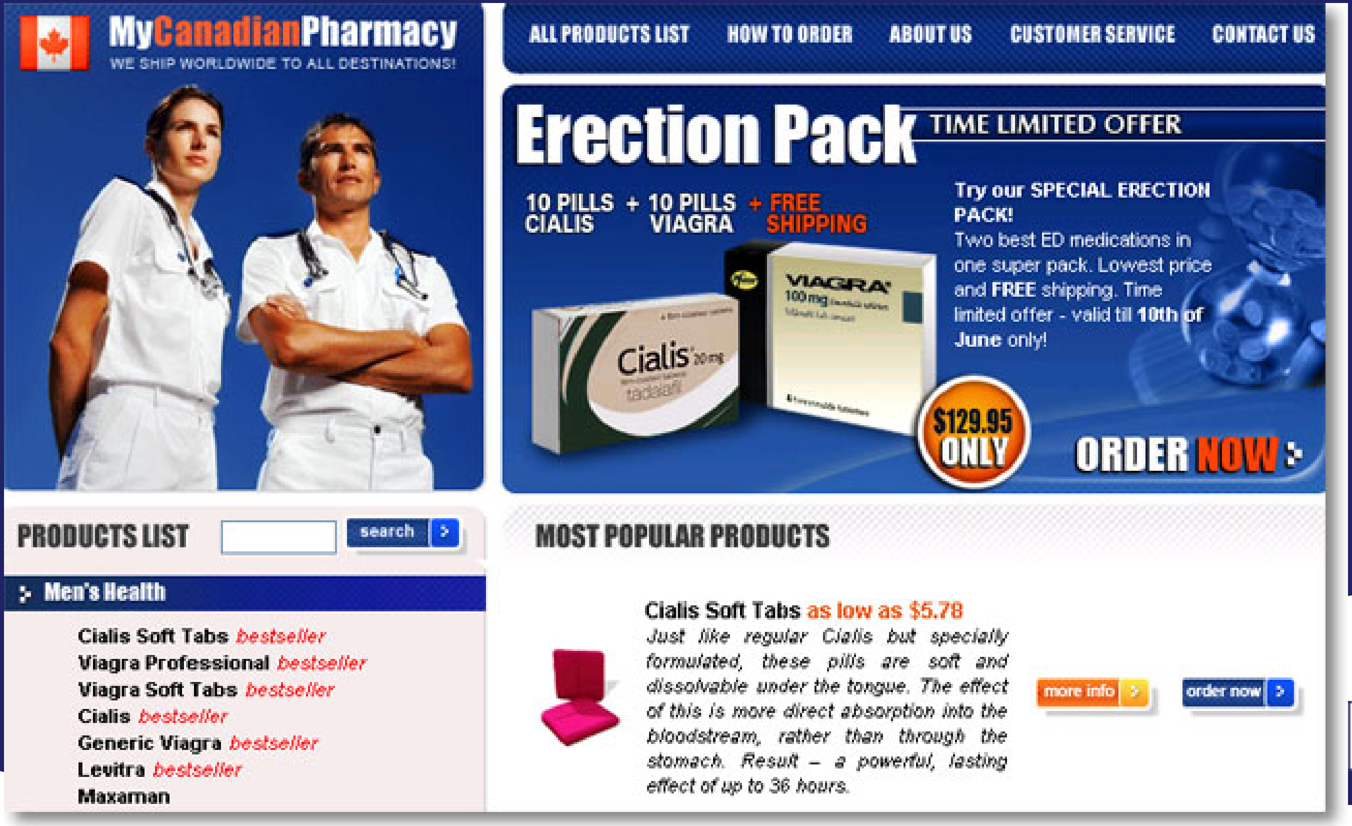
Cialis Soft Tabs as low as $5.78

Just like regular Cialis but specially formulated, these pills are soft and dissolvable under the tongue. The effect of this is more direct absorption into the bloodstream, rather than through the stomach. Result – a powerful, lasting effect of up to 36 hours.

July 11-12, 2007
SPAM SUMMIT

4. Customer Response Infrastructure

- Spammers need the recipient to **take action**
- Usually use a webserver but can also use a phone number, email address or stock trading system



Try our SPECIAL ERECTION PACK! Two best ED medications in one super pack. Lowest price and FREE shipping. Time limited offer - valid till **10th of June** only!

- Cialis Soft Tabs *bestseller*
- Viagra Professional *bestseller*
- Viagra Soft Tabs *bestseller*
- Cialis *bestseller*
- Generic Viagra *bestseller*
- Levitra *bestseller*
- Maxaman

Cialis Soft Tabs as low as $5.78

Just like regular Cialis but specially formulated, these pills are soft and dissolvable under the tongue. The effect of this is more direct absorption into the bloodstream, rather than through the stomach. Result – a powerful, lasting effect of up to 36 hours.

Web site requirements

1. Register domain
2. DNS server
3. Publish two DNS records
    - NS record – find the DNS server
    - A record – find the web server
4. Web server
5. Load content onto web server

MyCanadianPharmacy Example

1. Registered domain **bigamousetract.info**
   - Registered with 1-877namebid.com
   - Registered by Tobyann Ellis in Longview, WA, +68 phone number and dublin.com email
2. DNS servers
   - ‘NS’ Records point to DNS servers in Taiwan, Spain, US, Brazil
   - ‘A’ Record for web server points to Korean Telecom IP
3. Web server
   - **bigamousetract.info** server on Korean Telecom network
   - Web site images from Brazil, Slovenia, France, Greece, Netherlands

Note: Spammers use multiple methods to obfuscate web site connection including redirectors, framing, scripting, reverse proxies, zombie proxies

5. Payments
6. Fulfillment

5. Payment Processing

- Obtain money from victims

6. Fulfillment

- Customer service, sourcing, shipping

Evolving Methods for Sending Spam and Malware

- **Ben Butler,** Director of Network Abuse, GoDaddy.com, Inc.
- **Patrick Peterson,** Vice President, Technology, IronPort Systems
- **Jon L. Praed, Esq.,** Partner, Internet Law Group
- **Suresh Ramasubramanian,** Manager, Antispam Operations, Outblaze Limited
- **Joe St Sauver, Ph.D.,** Manager, Internet2 Security Programs, Internet2 and the University of Oregon

SPAM SUMMIT July 11-12, 2007

Joe St. Sauver, Ph.D

- Manager, *Internet2 Security Programs, Internet2* and the *University of Oregon***

- *** Affiliation information provided for identification purposes only; all opinions expressed are solely those of the presenter and do not necessarily represent those of any organization*

SPAM SUMMIT July 11-12, 2007

Evolving Methods for Sending Spam and Malware: Spammer Requirements and the Spam Ecosystem

FTC Spam Summit: The Next Generation of Threats and Solutions, July 11-12th, 2007, Washington DC

Joe St Sauver, Ph.D. (joe@uoregon.edu or joe@internet2.edu)

Manager, Internet2 Security Programs, Internet2/U of Oregon

http://www.uoregon.edu/~joe/spam-summit/

Disclaimer: all opinions expressed in this presentation are strictly the author's, and do not necessarily represent those of any other organization or entity.

July 11-12, 2007 SPAM SUMMIT

The evolution of spam: it ISN'T exclusively a "technology thing" anymore

- While it would be easy to focus **exclusively** on evolving technological spam phenomena (such as the move toward sending image spam to avoid SURBL filters, or emergence of fast flux hosting as a phenomena), **the evolution of spam and spamming ISN'T just a "technology thing."** Spam is also evolving at "strategic" and "business" levels.
- For example, illegitimate **affiliate programs** allow spammers to efficiently scale up/"franchise" their operations horizontally while also providing additional "insulation" from prosecution ("hey, I ***told*** my affiliates not to spam!").
- In fact, we're seeing the emergence of a specialized **"spam ecosystem,"** comprised of specialized suppliers of goods and services for spamming. Result? Higher efficiency & a lower bar to entry (buy rather than build what's needed), etc.

That ecosystem is complex (AND vulnerable!)

- Because spamming is an increasingly sophisticated, complex and collaborative activity, it largely isn't something which a spammer can learn and then do on their own anymore. New spammers need to comprehend a continually expanding body of operational techniques **("spam tradecraft")** in order to efficiently deliver spam while avoiding filtering, civil suits and criminal prosecution.
- Learning that spammer tradecraft, and doing routine spam-related business, requires spammers to **communicate** with with others spammers, and with spam support businesses. Monitoring those communications (with appropriate court permission) may make it possible for LE to use traffic analysis to identify participants in spammer organizations.
- Spammers also need to make **purchases** of spam-related goods & services (colocation space, etc.), potentially leaving behind incriminating financial records for forensic review.

Following that money trail

- The U.S. Money Laundering Threat Assessment Working Group did an great job of describing the financial channels which miscreants exploit; I'd urge everyone to review the Dec. '05 **U.S. Money Laundering Threat Assessment,** http://www.ustreas.gov/offices/enforcement/pdf/mlta.pdf
- Not surprisingly, in view of that scrutiny, financial choke points are beginning to emerge. Spammer **payment processing** is a prime example of this. For example, at least in the case of one popular pharma spammer, only **one** type of credit cards can still be used by customers to pay for illegal controlled substances. Identify a way to break THAT financial channel, and spammers will be badly damaged.
- Or scrutinize the payments made by affiliate programs to their participating affiliates. Are **income tax liability issues** associated with that income stream being properly handled?

Follow the product (order fulfillment)

- If you're chasing connections between spam, spammers and spamvertised products, don't forget that spammers need to get spamvertised products to customers -- unless spammers are just directly defrauding their customers. (After all, if a spammer **does** rip off a customer, would the customer really complain to local police that they're not receiving the illegal controlled substances they've purchased online?)
- Assuming spammers **are** delivering some products which people order, those products are getting **shipped** from somewhere, probably via a major common carrier. Records/ patterns are being created–but is anyone looking at them?
- There are no borders in cyberspace, but there **ARE** borders in real life. When spammers ship illegal drugs from abroad, those shipments go through **customs**. If you want to disrupt pillz spammers, seizing shipments at the border is a great step – but does Customs (and DEA) have the needed staff?

Spammers and anonymity

- As spammers see things like financial and fulfillment channels being successfully attacked by law enforcement, not surprisingly, spammers adapt. That's one reason why smarter spammers now prefer to spam things which can't be directly tied back to them, such as **stock pump and dump spam**, or **mortgage lead spam**. Spammers are looking for insulation. Spammers are looking for anonymity.
- There are plenty of things which help spammers in their quest for anonymity, including:
  -- anonymized domain registrations (to say nothing of the ongoing problem of <u>completely</u> bogus whois contact data)
  -- cheap/easy-to-create offshore shell corporations,
  -- national privacy laws (particularly in some parts of the EU)
     which interfere with even voluntary action by ISPs to
     protect their own facilities/customers from exploitation, &
  -- primitive mechanisms for international LE
  cooperation.

Spam: it *IS* an INTERNATIONAL phenomena

- As the United States cracks down on spam, spammers are developing an increasingly strong affinity for Europe, including living in Europe, exploiting European consumer PCs to send spam to United States email addresses, etc.
- Because spam is an international phenomenon, dealing with spam will require a coordinated **international response**.
  It doesn't help much if we clean up all our domestic spam zombies, if we're still getting hammered by spam sent through Poland or Spain, or if spammers have a safe base of operations in Russia or elsewhere overseas.
- Some may even go so far as to describe spam as a sort of low-intensity cyber warfare conducted via third parties. **How much in aggregate has the US economy been damaged by spam?** What a "perfect" way for those who hate the US to safely attack our economy! We may not even notice we're being attacked, and if we did, how would we respond?

Six Quick Closing Thoughts

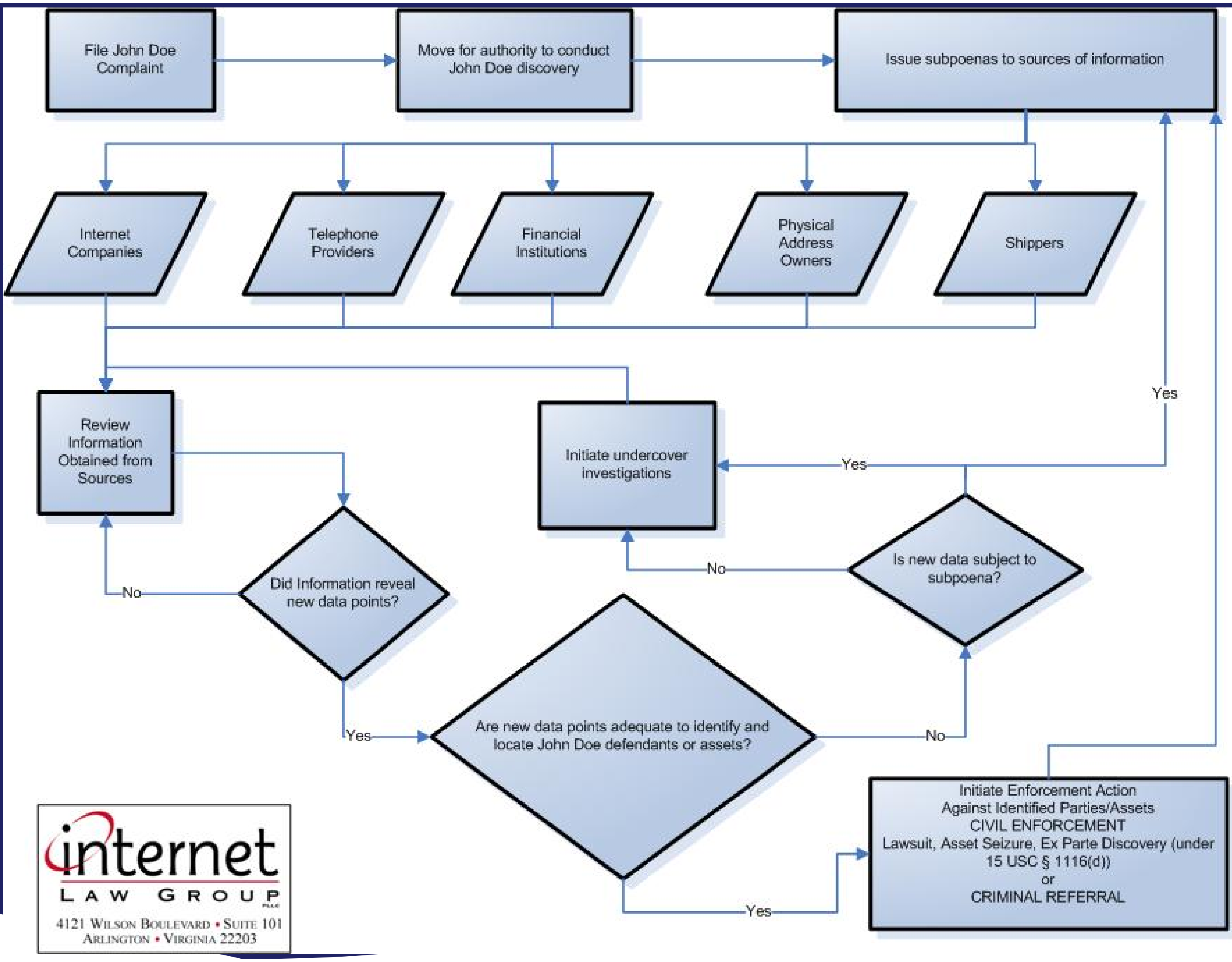
- 1. The Internet is a gigantic laboratory for spammers. They can easily try new approaches and see what works. While we can and must respond to any and all of those new approaches, we're never going to win if we just play a defensive game since it always take time to develop and deploy countermeasures. **We need to go on the offense.**
- 2. **Spamming requires a lot of "stuff."** Spamming is not a lightweight activity, and there's a substantial specialized industry of folks who've grown up around spamming, all doing business supporting it. ALL of those cottage industries can and SHOULD be targeted for investigative attention.
- 3. **Choke points exist, and they need to be worked relentlessly.** Merchant account processing and interdiction of illegal shipments at our borders are excellent examples of these weaknesses.

- 4. **Spamming activity doesn't occur in isolation.** For example, spam senders communicate with, and are paid by, affiliate programs. If you can bust spam senders you can use them to identify affiliate programs; if you bust affiliate programs, you can use them to work back to spam senders. When you uncover one thread, follow it to find all the rest of the operation, and offer deals (including immunity from prosecution) to get the little guys to roll over on the big guys.
- 5. The bad guys have learned one key lesson of the Internet: they're doing an excellent job of **scaling up** their operations, with affiliate programs being a prime example. Does the U.S. **also** have plans to **scale up** *its* **anti-spam** operations? **What's next, post CAN-SPAM?**
- 6. Spam is an **international problem** and one which will require a coordinated **international response** if we're going to win. The United States must show international leadership and support for international antispam efforts.

Jon L. Praed, Esq.

- Partner, *Internet Law Group*

Civil Spam Discovery Process



File John Doe Complaint

Move for authority to conduct John Doe discovery

Issue subpoenas to sources of information

Internet Companies

Telephone Providers

Financial Institutions

Physical Address Owners

Shippers

Review Information Obtained from Sources

Did Information reveal new data points?

Initiate undercover investigations

Is new data subject to subpoena?

Are new data points adequate to identify and locate John Doe defendants or assets?

Initiate Enforcement Action
Against Identified Parties/Assets
CIVIL ENFORCEMENT
Lawsuit, Asset Seizure, Ex Parte Discovery (under 15 USC § 1116(d))
or
CRIMINAL REFERRAL

internet
LAW GROUP PLLC
4121 Wilson Boulevard • Suite 101
Arlington • Virginia 22203

July 11-12, 2007
SUMMIT

Evolving Methods for Sending Spam and Malware

- **Ben Butler,** Director of Network Abuse, GoDaddy.com, Inc.
- **Patrick Peterson,** Vice President, Technology, IronPort Systems
- **Jon L. Praed, Esq.,** Partner, Internet Law Group
- **Suresh Ramasubramanian,** Manager, Antispam Operations, Outblaze Limited
- **Joe St Sauver, Ph.D.,** Manager, Internet2 Security Programs, Internet2 and the University of Oregon

LUNCH

Lunch (On your Own):

12:30 PM - 1:45 PM